(12)特許協力条約に基づいて公開された国際出願

(19) 世界知的所有権機関
国際事務局

(43) 国際公開日
2004 年5 月13 日 (13.05.2004)

PCT

(10) 国際公開番号
WO 2004/040902 A1

(51) 国際特許分類[7]: H04N 1/387

(21) 国際出願番号: PCT/JP2003/013772

(22) 国際出願日: 2003 年10 月28 日 (28.10.2003)

(25) 国際出願の言語: 日本語

(26) 国際公開の言語: 日本語

(30) 優先権データ:
特願2002-315391 2002 年10 月30 日 (30.10.2002) JP

(71) 出願人 (米国を除く全ての指定国について): 独立行政法人科学技術振興機構 (JAPAN SCIENCE AND TECHNOLOGY AGENCY) [JP/JP]; 〒332-0012 埼玉県 川口市 本町 4－1－8 Saitama (JP).

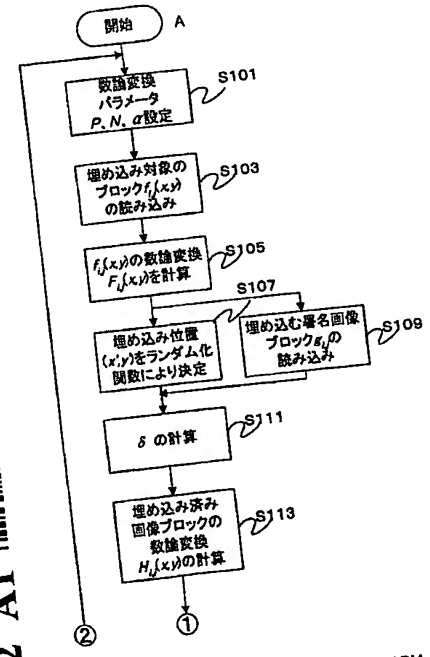
(72) 発明者; および
(75) 発明者/出願人 (米国についてのみ): 青木 直史 (AOKI,Naofumi) [JP/JP]; 〒063-0059 北海道 札幌市西区 宮の沢２条１丁目１－３０－１３１０ Hokkaido (JP). 田森 秀明 (TAMORI,Hideaki) [JP/JP]; 〒062-0033 北海道 札幌市豊平区 西岡３条１０丁目１－２０ Hokkaido (JP). 山本 強 (YAMAMOTO,Tsuyoshi)

[続葉有]

(54) Title: FALSE ALTERATION DETECTING METHOD, FALSE ALTERATION DETECTING PROGRAM, AND RECORDED MEDIUM ON WHICH THE PROGRAM IS RECORDED

(54) 発明の名称: 改ざん検出方法、改ざん検出プログラム及びそのプログラムを記録した記録媒体

WO 2004/040902 A1



A...START
S101...SET NUMBER THEORETIC TRANSFORM PARAMETERS P, N, α
S103...READ BLOCKS $f_{i,j}(x,y)$ TO BE EMBEDDED
S105...CALCULATE NUMBER THEORETIC TRANSFORM $F_{i,j}(x,y)$ OF $F_{i,j}(x,y)$
S107...DETERMINE EMBEDMENT POSITION (x',y') BY USING RANDOMIZING FUNCTION
S109...READ SIGNATURE IMAGE BLOCK $g_{i,j}$ TO BE EMBEDDED
S111...CALCULATE δ
S113...CALCULATE NUMBER THEORETIC TRANSFORM $H_{i,j}(x,y)$ OF EMBEDDED IMAGE BLOCK

(57) Abstract: A false alteration detecting method using an electronic watermark method of fragile type by number theoretic transform. A processing section sets parameters P, N, α of number theoretic transform (S101), and reads original image blocks $f_{i,j}(x,y)$ (S103), conducts number theoretic transform of $f_{i,j}(x,y)$ to calculate the number theoretic transform blocks $F_{i,j}(x,y)$ (S105), determines the position (x', y') at which a signature image is to be embedded by using a randomizing function (S107), reads pixel values $g_{i,j}$ of the signature image for embedment from a storage section (S109), determines the embedment value δ of each block from the $F_{i,j}(x', y')$ of the embedment position and $g_{i,j}$ (S111), adds the embedment value δ to the $F_{i,j}(x,y)$ or subtracts the embedment value δ from the $F_{i,j}(x,y)$ to determine the number theoretic transform blocks $H_{i,j}(x,y)$ of the embedded image block (S113), calculates the inverse number theoretic transform of the $H_{i,j}(x,y)$, determines the embedded image blocks $h_{i,j}(x,y)$, stores them, and outputs them to an output section.

(57) 要約: 数論変換による脆弱型の電子透かし法を用いた改ざん検出法。 処理部は、数論変換のパラメータＰ、Ｎ、αを設定し（Ｓ１０１）、原画像ブロック $f_{i,j}$（ｘ、ｙ）を読み込む（Ｓ１０３）。処理部は、$f_{i,j}$（ｘ、ｙ）を数論変換して数論変換ブロック $F_{i,j}$（ｘ、ｙ）を計算する（Ｓ１０５）。処理部は、署名画像の埋め込み位置（ｘ'、ｙ'）をランダム化関数に基づき決定し（Ｓ１０７）、埋め込むための署名画像の画素値 $g_{i,j}$ を記憶部から読み込む（Ｓ１０９）。処理部は、埋め込み位置の $F_{i,j}$（ｘ'、ｙ'）と $g_{i,j}$ とにより、各ブロックの埋め込み量δを求め（Ｓ１１１）、$F_{i,j}$（ｘ、ｙ）に埋め込み量δを加算又は減算して、埋め込み済み画像ブロックの数論変換ブロック $H_{i,j}$（ｘ、ｙ）を求める（Ｓ１１３）。処理部は、$H_{i,j}$（ｘ、ｙ）の逆数論変換を計算して、埋め込み済み画像ブロック $h_{i,j}$（ｘ、ｙ）を求め、それを記憶し、出力部等に出力する。

[JP/JP]; 〒064-0804 北海道 札幌市中央区 南４条西１１丁目１２９３−１２−８０５ Hokkaido (JP).

(74) 代理人: 橋爪 健 (HASHIZUME,Takeshi); 〒104-0061 東京都 中央区 銀座３丁目１３番１７号 Tokyo (JP).

(81) 指定国 (国内): CN, KR, US.

(84) 指定国 (広域): ヨーロッパ特許 (DE, FR, GB).

添付公開書類:
— 国際調査報告書

明 細 書

改ざん検出方法、改ざん検出プログラム及びそのプログラムを記録した記録媒体

技術分野

本発明は、改ざん検出方法、改ざん検出プログラム及びそのプログラムを記録した記録媒体に係り、特に、数論変換による脆弱型電子透かしを用いた画像の改ざん位置検出技術に関する。

背景技術

一般に、証拠写真などの公文書で用いられる画像には原本性が十分に保証されたものが要求されるが、ディジタル画像は不自然さを排除した改ざんを比較的容易に行えるため、その証拠能力が不十分な場合がある。ゆえに、ディジタル画像における原本性保証や改ざん検出の技術が求められている。従来、これらの目的を実現する方法としてハッシュ関数を用いた電子署名が検討されてきた。しかし、電子署名は改ざんの位置検出をすることを意図していない。

そこで、従来より改ざん位置検出を行う一つの方法として電子透かしが注目されている。電子透かしはその性質に応じて耐性型と脆弱型との二種類に分類される。耐性型電子透かしは攻撃に対してロバストな性質を持ち、主に著作権保護を目的とする場合に用いられる。一方、改ざん位置検出には脆弱型電子透かしを使用する。脆弱型電子透かしは画像処理に対して非常に敏感に反応する性質を持つ。改ざん検出の過程において、何らかの変化を生じている電子透かしを同定することで改ざんの位置を特定できる。以下に参照文献リストを示す。

特開2002－44429号公報

特開2002－201703号公報

田森秀明、青木直史、山本強、“数論変換を用いた改ざん検出可能な電子透かし方式” 電子情報通信学会技術研究報告 IE2001-33,pp.105-110, Jul. 2001.

田森秀明、青木直史、山本強、“数論変換による脆弱型電子透かしを用いた静止画像の改ざん位置検出と改ざん訂正” 電子情報通信学会技術研究報告 IE2002-45,pp.19-24, Jul. 2002.

H. Tamori, N. Aoki, and T. Yamamoto, “A Fragile Digital Watermarking Technique by Number Theoretic Transform,” IEICE Trans. Fundamentals, Aug.2002.

発明の開示

以上のような改ざん位置検出を目的とした脆弱型電子透かしの従来手法としては、ディジタルコンテンツから得られたハッシュ値やパリティ値をビットプレーンに埋めるといったものが主であった。しかしながらこれらの手法はアルゴリズム公開時の安全性に問題がある場合があり、例えば複数の異なる埋め込み済み画像から改ざん画像を合成するような、特定の改ざんは検出できなかった。

一方、耐性型電子透かしにおいては、離散フーリエ変換などの直交変換を利用した、比較的安全性の高い手法が数多く提案されている。そのような耐性型電子透かしの手法を脆弱型電子透かしに応用することで安全性の更なる向上が期待できると考えられる。そこで本発明者等は数論変換（number theoretic transform: NTT）と呼ばれる直交変換を用いた脆弱型電子透かし法を検討してきた。数論変換は、系列に与えられた変化がわずかでも、その変換結果が変化を与える前に比べ大きく異なるという脆弱な性質を持つ。

本発明は、以上の点に鑑み、直交変換を用いた耐性型電子透かし法を応用した数論変換による脆弱型の電子透かし法を用いた改ざん検出方法、改ざん検出プログラム及びそのプログラムを記録した記録媒体を提案することを目的とする。また、本発明は、改ざんの有無及びその位置を目視によって容易に確認することができる改ざん検出法等を提供することを目的とする。

さらに、従来の数論変換を利用した電子透かしの手法では、原画像の画像ビットを下位2bit程度という比較的少ない範囲で置換することにより署名情報を埋め込むものであった。これに対して、本発明では、原画像の画素ビットの全て又は所望の広範囲を利用して署名情報を埋め込むことにより安全性を一層高めることを目的とする。また、従来の数論変換を利用した手法では、署名情報の埋め込みを数論変換ドメインに掛け合わせて(畳み込んで)実現していた。これに対して、本発明では、署名情報の埋め込みを足し算により実現することで、演算速度を速くすることを目的とする。

本発明の第1の解決手段によると、

処理部は、数論変換のパラメータである法P、位数N、根αを設定するステップと、

処理部は、記憶部から、埋め込み対象の原画像[f]をブロック分割した原画像ブロック$f_{i,j}(x,y)$を読み込むステップと、

処理部は、設定された法P、位数N、根αを用いて、原画像ブロック$f_{i,j}(x,y)$を数論変換して原画像ブロックの数論変換ブロック$F_{i,j}(x,y)$を計算するステップと、

処理部は、各ブロックにおける署名画像の埋め込み位置(x'、y')を、所定のランダム化関数に基づき決定するステップと、

処理部は、埋め込むための署名画像の画素値$g_{i,j}$を記憶部から読み込むステップと、

処理部は、埋め込み位置の原画像ブロックの数論変換ブロック$F_{i,j}(x',y')$と署名画像の画素値$g_{i,j}$と埋め込み強度εにより、各ブロックの埋め込み量δを求めるステップと、

処理部は、原画像ブロックの数論変換ブロック$F_{i,j}(x,y)$に、(x、y)に応じて埋め込み量δを加算又は減算して、埋め込み済み画像ブロックの数論変換ブロック$H_{i,j}(x,y)$を求めるステップと、

処理部は、数論変換ブロック$H_{i,j}(x,y)$の逆数論変換を計算して、埋め込み済み画像ブロック$h_{i,j}(x,y)$を求めるステップと、

処理部は、全ての又は所望の範囲の(i, j)ブロックについて埋め込み済み画像ブロック$h_{i,j}(x,y)$を求めることにより埋め込み済み画像[h]を得て、それを記憶部に記憶する、及び／又は、出力部若しくはインターフェースにより出力するステップと

含む改ざん検出方法、これら各ステップをコンピュータに実行させるための改ざん検出プログラムを記録した記録媒体が提供される。

本発明の第2の解決手段によると、

処理部は、埋め込み済み画像[h]をブロック分割した埋め込み済み画像ブロック$h_{i,j}(x,y)$を、記憶部又は入力部又はインターフェースから読み込むステップと、

処理部は、数論変換のためのパラメータである法P、位数N、根αを設定するステップと、

処理部は、埋め込み済み画像ブロック$h_{i,j}(x,y)$を数論変換して埋め込み済み画像ブロックの数論変換ブロック$H_{i,j}(x,y)$を計算するステップと、

処理部は、署名画像の埋め込み位置に対応する抽出位置(x'、y')を所定のランダム化関数に基づいて決定するステップと、

処理部は、抽出位置の数論変換ブロック$H_{i,j}(x',y')$の埋め込み強度εによる剰余を取ることによって、署名画像の画素値$g_{i,j}$を抽出するステップと、

処理部は、全ての又は所望の範囲の(i, j)ブロックについて署名画像の画素値$g_{i,j}$を求めることにより署名画像[g]を得て、それを記憶部に記憶する、及び／又は、表示部若しくは出力部若しくはインターフェースに出力するステップと

含む改ざん検出方法、これら各ステップをコンピュータに実行させるための改

ざん検出プログラムを記録した記録媒体が提供される。

本発明の第3の解決手段によると、

署名画像を原画像に埋め込む処理及び署名画像を抽出する処理を含む改ざん検出方法であって、

前記埋め込む処理は、

処理部は、数論変換のパラメータである法P、位数N、根αを設定するステップと、

処理部は、記憶部から、埋め込み対象の原画像[f]をブロック分割した原画像ブロック$f_{i,j}(x,y)$を読み込むステップと、

処理部は、設定された法P、位数N、根αを用いて、原画像ブロック$f_{i,j}(x,y)$を数論変換して原画像ブロックの数論変換ブロック$F_{i,j}(x,y)$を計算するステップと、

処理部は、各ブロックにおける署名画像の埋め込み位置(x'、y')を、所定のランダム化関数に基づき決定するステップと、

処理部は、埋め込むための署名画像の画素値$g_{i,j}$を記憶部から読み込むステップと、

処理部は、埋め込み位置の原画像ブロックの数論変換ブロック$F_{i,j}(x',y')$と署名画像の画素値$g_{i,j}$と埋め込み強度εにより、各ブロックの埋め込み量δを求めるステップと、

処理部は、原画像ブロックの数論変換ブロック$F_{i,j}(x,y)$に、(x、y)に応じて埋め込み量δを加算又は減算して、埋め込み済み画像ブロックの数論変換ブロック$H_{i,j}(x,y)$を求めるステップと、

処理部は、数論変換ブロック$H_{i,j}(x,y)$の逆数論変換を計算して、埋め込み済み画像ブロック$h_{i,j}(x,y)$を求めるステップと、

処理部は、全ての又は所望の範囲の(i, j)ブロックについて埋め込み済み画像ブロック$h_{i,j}(x,y)$を求めることにより埋め込み済み画像[h]を得て、それを記憶部に記憶する、及び／又は、出力部若しくはインターフェースにより出力するステップと

を含み、

前記抽出処理は、

処理部は、埋め込み済み画像[h]をブロック分割した埋め込み済み画像ブロック$h_{i,j}(x,y)$を、記憶部又は入力部又はインターフェースから読み込むステップと、

処理部は、数論変換のためのパラメータである法P、位数N、根αを設定するステップと、

処理部は、埋め込み済み画像ブロック$h_{i,j}(x,y)$を数論変換して埋め込み済み画像ブロックの数論変換ブロック$H_{i,j}(x,y)$を計算するステップと、

処理部は、署名画像の埋め込み位置に対応する抽出位置(x'、y')を所定のランダム化関数に基づいて決定するステップと、

処理部は、抽出位置の数論変換ブロック$H_{i,j}(x',y')$の埋め込み強度εによる剰余を取ることによって、署名画像の画素値$g_{i,j}$を抽出するステップと、

処理部は、全ての又は所望の範囲の(i, j)ブロックについて署名画像の画素値$g_{i,j}$を求めることにより署名画像[g]を得て、それを記憶部に記憶する、及び／又は、表示部若しくは出力部若しくはインターフェースに出力するステップと

含む改ざん検出方法、これら各ステップをコンピュータに実行させるための改ざん検出プログラムを記録した記録媒体が提供される。

図面の簡単な説明

第1図は、素数13の$y^x \pmod{13}$の説明図である。

第2図は、システム構成の概略図である。

第3図は、改ざん位置検出装置の構成図である。

第4図は、離散フーリエ変換による電子透かし法についての説明図である。

第5図は、数論変換による脆弱型電子透かし法についての説明図である。

第6図は、埋め込み処理のフローチャート(1)である。

第7図は、埋め込み処理のフローチャート(2)である。

第8図は、埋め込みによる画素値への影響についての説明図である。

第9図は、抽出処理のフローチャートである。

第10図は、実験に使用する画像の図である。

第11図は、実験結果の画像の図(1)である。

第12図は、出力画像の画質と埋め込み強度εの関係である。

第13図は、実験結果の画像の図(2)である。

発明を実施するための最良の形態

1. 数論変換

1.1 概要

はじめに、数論変換について説明する。なお、数論変換については、必要であれば以下の文献を参照のこと。

- J. H. McClellan, and C. M. Rader, "Number Theory in Digital Signal Processing," Prentice-Hall, New Jersey, 1979.
- 電子情報通信学会(編)、ディジタル信号処理ハンドブック、オーム社、東京、1993.
- S. C. Coutinho(著)、林彬(訳)、暗号の数学的基礎、シュプリンガー・フェアラーク東京株式会社、東京、2001.
- H. J. Nussbaumer(著)、佐川雅彦、本間仁志(訳)、高速フーリエ変換のアルゴリズム、科学技術出版社、東京、1989.
- 谷荻隆嗣(著)、ディジタル信号処理ライブラリー4 アルゴリズムと並列処理、コロナ社、東京、2000.
- 青木由直、波動信号処理、森北出版、東京、1986

まず、パラメータP、αを正の整数、Nを$\alpha^N = 1 \bmod P$となる最小の正の整数とする。ここで、φ(P)をEuler関数とすると、N=φ(P)となるαを位数Nの原始根と呼び、N<φ(P)のαを、単に位数Nの根と呼ぶ。なお、φ(P)は、Pよ

り小さく、かつPに対し互いに素となる整数の個数を表す。

ここで、αを用いた次のような変換対を考える。

$$X(k) = \sum_{n=0}^{N-1} x(n)\alpha^{kn} \pmod{P} \quad (1)$$

$$x(n) = \frac{1}{N}\sum_{k=0}^{N-1} X(k)\alpha^{-kn} \pmod{P} \quad (2)$$

上式の計算は、Pを法とする剰余数系ですべての演算が可能なため、丸め誤差を一切生じない。電子透かしへの応用を考えたとき、Pを秘匿しておけば、数論変換の性質から、第三者は期待する変換結果を得ることができないため、Pは鍵情報として利用できる。ところで、数論変換においてはPには、メルセンヌ数やフェルマー数を用いるのが代表的である(例えば、電子情報通信学会(編)、ディジタル信号処理ハンドブック、オーム社、東京、1993 等参照。)。しかしながら、これらには厳しい制限があり、選択できる数が少なく鍵情報として用いるのには不適当な場合があった。そこで、Pが素数のべき上による任意の合成数でも可能である手法を適用する。

pを素数として、

$$P = p_1^{r1} p_2^{r2} \cdots p_m^{rm} \quad (3)$$

で表されるとする。まず、位数Nを

$$N|\mathrm{GCD}[(p_1 - 1), (p_2 - 1), \cdots, (p_m - 1)] \quad (4)$$

を満たす正の整数から選択する。p_mを法とする位数Nの根$\alpha_{1,m}$を計算し、次に位数Nの根$\alpha_{2,m}$を

$$\alpha_{2,m} = \alpha_{1,m}^{p_m^{r_m-1}} \pmod{p_m^{r_m}} \qquad (5)$$

で求める。続いて中国剰余定理により$\alpha_{2,m}$からPを法とする位数Nの根αを求めることができる(例えば、H. J. Nussbaumer(著)、佐川雅彦、本間仁志(訳)、高速フーリエ変換のアルゴリズム、科学技術出版社、東京、1989 等参照。)。

一般に、剰余系で演算を行う場合取扱える数の範囲を広げるため、異なる法の剰余系の組を用い、演算結果は法ごとの結果の組となる場合がある。中国剰余定理(Chinese remainder theorem)は、この組からある進数で唯一に定まる数を求めるもので次のように表わせる。(青木由直「波動信号処理」、森北出版株式会社、1986年4月3日、参照)

[定理] 法m_i(i=1、2、・・・、l)を互いに素な正整数に選びM=$m_1m_2\cdots m_l$とすると

$<a>_{mi}=r_i$ (i=1、2、・・・、l)

(ここに、r_iは法m_iに関するaの剰余である。)

を満足する正整数a(0<a≦M−1)は次式で唯一に与えられる。

$a=\Sigma d_i d_i^{-1} r_i \pmod{M}$

ここで、

Σは、i=1～lの和

$d_i=M/m_i$ 、

$d_i^{-1}=(<d_i>_{mi})^{-1} \pmod{m_i}$

(なお、$(<d_i>_{mi})^{-1}$は法m_iでの乗法逆元。)

1.2 例

例えば、P=61009=$13^2\times19^2$による数論変換を考える。まず、GCD[12、18]=6より、NをN | 6=[1、2、3、6]から選択する。ここではN=3を採用す

る。次に13と19を法とする位数3の根を計算する。それぞれを$\alpha_{1,1}$、$\alpha_{1,2}$とすると、$\alpha_{1,1}=3$、$\alpha_{1,2}=7$である。よって、13^2と19^2を法とする位数3の根を$\alpha_{2,1}$、$\alpha_{2,2}$とすると、次のようになる。

$$\alpha_{2,1} = 3^{13^2-1} = 146 \pmod{13^2}$$

$$\alpha_{2,2} = 7^{19^2-1} = 292 \pmod{19^2}$$

続いて、よく知られた中国剰余定理により、61009を法とする位数3の根は$\alpha=653$と求まる。

図1に、素数13のy^x(mod 13)の説明図を示す。

例えば、13を法とする位数3の根の見つけ方を考える。yが縦、xが横である。1が出る周期がNである時、yを13を法とした位数N(ここだと3)である。y=3、9の時、3つおきに"3"が出ているため、3、9が根である。ここでは、例えば、複数の根のうち最小のものを選択することとすると、根=3となる。なお、数論の全般的なことについては、

http://fox.zero.ad.jp/~zat25960/math/number/index.htm 等参照。

ここで、一例として、以上に基づき、N=3の系列$x=[10、20、30]^T$の数論変換を考える。式(1)、(2)は行列表示すると次のようになる。

$X=[T]x$

$x=[T]^{-1}X$

ただし、

$X=[X(0)、X(1)、X(2)]^T$

$x=[x(0)、x(1)、x(2)]^T$

である。変換行列[T]は、

$$[T] = [\alpha^{kn}] = \begin{bmatrix} 1 & 1 & 1 \\ 1 & 653 & 653^2 \\ 1 & 653^2 & 653^4 \end{bmatrix}$$
$$= \begin{bmatrix} 1 & 1 & 1 \\ 1 & 653 & 60355 \\ 1 & 60355 & 653 \end{bmatrix} \pmod{61009}$$

となり、逆変換行列[T]$^{-1}$は

$$[T]^{-1} = N^{-1}[\alpha^{-kn}]$$
$$= 3^{-1} \begin{bmatrix} 1 & 1 & 1 \\ 1 & 653^{-1} & 653^{-2} \\ 1 & 653^{-2} & 653^{-4} \end{bmatrix}$$
$$= \begin{bmatrix} 40673 & 40673 & 40673 \\ 40673 & 60791 & 20554 \\ 40673 & 20554 & 60791 \end{bmatrix} \pmod{61009}$$

となる。xを数論変換すると、

$$\mathbf{X} = \begin{bmatrix} 1 & 1 & 1 \\ 1 & 653 & 60355 \\ 1 & 60355 & 653 \end{bmatrix} \cdot \begin{bmatrix} 10 \\ 20 \\ 30 \end{bmatrix}$$
$$= [60, 54459, 6520]^T \pmod{61009}$$

となり、[T]$^{-1}$を用いて逆変換すると、

x＝[T]$^{-1}$X＝[10、20、30]^{T}(mod 61009)

が得られる。

ここで、例えば、変換後の系列X＝[60、54459、6520]^{T}がX'＝[61、54459、6521]^{T}に改ざんされたとする。逆変換後の出力x'は、

x'＝[T]$^{-1}$X'＝[11、238、40485]^{T}(mod 61009)

となり、xとは全く異なる。この結果は、丸め誤差の生じない数論変換の性質か

ら得られるもので、改ざん検出に有効であるといえる。

2. ハードウェア

図2に、システム構成の概略図を示す。このシステムでは、送信者用コンピュータ10、受信者用コンピュータ20、認証機関用コンピュータ30を備える。送信者コンピュータ10から受信者用コンピュータ20へは署名情報が電子透かしで埋め込まれた画像情報[h]が伝達される。なお、署名データ[g]は送信者用コンピュータ10から受信者用コンピュータ20との間で予め決定されている。送信者用コンピュータ10から認証機関用コンピュータ30は鍵情報P、さらに、必要に応じて位数Nが送られる。受信者用コンピュータ20は認証機関用コンピュータ30からこれら鍵情報Pさらに、必要に応じてNを取得する。

上述のシステム構成以外にも、認証機関用コンピュータ30を省略して直接送信者用コンピュータ10と受信者用コンピュータ20との間で[h]、P、さらに必要によりNを送受信するようにしても良い。

送信者から受信者への[h]、P、Nの伝送手段は、例えば、次のような手段がある。ここで、[h]は公開してもかまわないため、受信者用コンピュータ20は送信者用コンピュータ10からe－mailで直接送信しても特に問題ないが、鍵情報Pは秘密鍵のため、送信者用コンピュータ10から受信者用コンピュータ20又は認証機関コンピュータ30に送信する場合にはセキュリティの観点から、RSAなどの暗号化を施した後に送信すると良い。例えば、ディジタルカメラでの運用を考えた場合、カメラから直接認証機関に送信されることが一案である。この場合はe－mailではなく、暗号化ファイルを直接パケット交換や回線交換で送信することもできる。これら鍵情報を受信者用コンピュータ20又は認証機関コンピュータ30から送信者用コンピュータ10が受信する場合も同様である。

図3は、改ざん位置検出装置の構成図である。

この装置は、中央処理装置（CPU）である処理部１、入力部２、出力部３、表示部４、記憶部５、インターフェース６を有する。また、処理部１、入力部２、出力部３、表示部４及び記憶部５は、スター又はバス等の適宜の接続手段で接続されている。記憶部５は、数論変換のパラメータを記憶する鍵ファイル５１、原画像[f]を記憶する原画像ファイル５２、署名画像ファイル[g]を記憶する署名画像ファイル５３、埋め込み済み画像ファイル[h]を記憶する埋め込み済み画像ファイル５４を含む。記憶部５は、さらに、後述するようなランダム化関数$r_{x'}$、$r_{y'}$、埋め込み強度εを予め記憶する。インターフェース６は、インターネット、移動体通信網等の各種ネットワークと接続され、他のコンピュータと情報の送受を無線、又は有線で行う。

３．改ざん位置検出

３．１　直交変換による耐性型電子透かし法

まず、参考として、離散フーリエ変換による電子透かし法の一例について説明する。

図４に、離散フーリエ変換による電子透かし法の一例についての説明図を示す。図（a）は、埋め込み処理について、図（b）は抽出処理について、それぞれ示す。

耐性型電子透かし法では、直交変換により得られた空間周波数領域に署名情報を埋め込む手法が数多く発表されている。そのような電子透かし法の一例として、図に示すような離散フーリエ変換を用いた手法について述べる。

埋め込み処理では、まず、処理部１は原画像[f]（KN×LN画素、8bit階調）をN×N画素のブロックに分割する。この分割した各ブロックを$f_{i,j}(x,y)$と表し、i、jは画像中でのブロックの位置を、x、yはブロック中での画素の座標を表す（i＝0、1、…、K－1；j＝0、1、…、L－1；x、y＝0、1、…、N－1）。次に、$f_{i,j}(x,y)$の２次元フーリエ変換を行い、この変換結果を$F_{i,j}(x,y)$で表す。

ここで、処理部1は、署名画像[g](K×L画素、1bit階調)を記憶部5から読み出すこと等により用意する。[g]の各画素値は$g_{i,j}$(=0又は1)とし、i、jは[g]の中での画素の座標を表すが、$f_{i,j}(x,y)$のi、jと対応する。処理部1は、$g_{i,j}$を$F_{i,j}(x,y)$の低周波成分に加え、埋め込み済みブロックのフーリエ変換$H_{i,j}(x,y)$を得る。つまり、εを埋め込み強度、(x'、y')を埋め込む要素の座標とすると、次式となる。

$$H_{i,j}(x,y)=\begin{cases}F_{i,j}(x,y)+\varepsilon g_{i,j} & x=x',y=y'\\ F_{i,j}(x,y) & \text{otherwise}\end{cases} \tag{6}$$

このとき、εと(x'、y')は、埋め込み処理と抽出処理であらかじめ共通にユーザが一意に設定しておけば、これらは埋め込み画像を抽出するための鍵となる。つぎに、処理部1は、$H_{i,j}(x,y)$を逆フーリエ変換し、埋め込み済みブロック$h_{i,j}(x,y)$を得る。処理部1は、以上の操作をすべてのブロックに行い、埋め込み済み画像[h]を得る。

一方、署名情報の抽出処理については、処理部1が、$H_{i,j}(x',y')$と$F_{i,j}(x',y')$の差分を取ることで実現する。つまり、次式により$g_{i,j}$を求める。

$$g_{i,j}=\varepsilon^{-1}\{H_{i,j}(x',y')-F_{i,j}(x',y')\} \tag{7}$$

以上のような手法では署名情報が低周波成分に埋め込まれていることから、多少の画像処理などの攻撃では署名情報は破壊されにくく、ロバストな手法となっている。このような理由から、直交変換によって得られる空間周波数領域を用いた手法は、著作権保護を目的とした耐性型電子透かし法に多く用いられている。

3．2 数論変換による脆弱型電子透かし法

図5に、数論変換による脆弱型電子透かし法についての説明図を示す。図(a)は、埋め込み処理について、図(b)は抽出処理について、それぞれ示す。

数論変換は離散フーリエ変換と同型の直交変換であるが、その変換領域には周波数領域のような物理的意味が無いため、上述の「3．1 直交変換による耐性型電子透かし法」をそのまま適用できない。また、上述3．1の手法では署名情報の抽出には原画像が必要なため、改ざん位置検出という目的では実用性に欠けることがある。ここでは、これらの課題を考慮した図示のような手法を提案する。

3．2．1． 埋め込み処理

図6及び図7に、埋め込み処理のフローチャート(1)及び(2)を示す。

埋め込み処理が開始されると、処理部1は、数論変換のパラメータである法P、及び位数N、根αを設定する(S101)。

Pは、例えば、あらかじめユーザが入力部2によって鍵ファイル51に設定するか、処理部1が熱雑音等を利用してランダムな値に決定することにより、処理前にあらかじめ鍵ファイル51に記憶しておく。処理部1は鍵ファイル51を参照してPを設定する。また、Pは、式(3)のように、素数のべき乗による任意の合成数を選択することができるが、剰余計算において画素値が取りうるすべての整数を扱うために、ここでは、処理部1は、一例として、画素値の最大値より大きな整数から選択する。

処理部1は、Pの決定後、式(4)に基づきNを選択する。処理部1は鍵ファイル51を参照するか、式(4)などを用いて計算することでNを設定する。Nは、あらかじめ入力部2により鍵ファイル51に記憶しておいても良いし、また、処理部1が、式(4)により、Pに依存した候補を求め、複数個の候補があるときはその中からいずれかを選択するようにしても良い。Nはブロックサイズであるので、大きすぎると正確な位置検出が出来ないことがあるので、一例としてN＝2、4

くらいが適当だと思われるが、これらはユーザが任意に選択するか、あらかじめシステムとして適当な選択方法を決定しておくことができる。

P、Nが決定されると、処理部1は、式(5)及び中国製剰余定理等により根αを計算することで、根αは一意に算出される。P、Nが未知である限り、後述する抽出処理が不可能であることから、P又はPとNの両方が、改ざん検出における鍵となる。

つぎに、処理部1は、記憶部5の原画像ファイル52から、原画像[f]をブロックに分割した埋め込み対象の原画像ブロック$f_{i,j}(x,y)$を読み込む(S103)。なお、上述と同様に原画像[f](KN×LN画素)をN×N画素のK×L個のブロックに分割し、この分割した各ブロックを$f_{i,j}(x,y)$と表し、i、jは画像中でのブロックの位置を、x、yはブロック中での画素の座標を表す(i=0、1、…、K−1;j=0、1、…、L−1;x、y=0、1、…、N−1)。

つぎに、処理部1は、式(1)、(2)に基づいて、ステップS101で設定したP、N、αを用いて、原画像ブロック$f_{i,j}(x,y)$を2次元数論変換された原画像ブロック$F_{i,j}(x,y)$を計算する(S105)。

つぎに、処理部1は、埋め込み済み画像ブロックの数論変換$H_{i,j}(x,y)$を、次式を用いて、以下に詳細に説明するように求める。

$$H_{i,j}(x,y) = F_{i,j}(x,y) + (-1)^{x+y}\delta \qquad (8)$$

ただし、δは式(9)を満たす、絶対値が最小の整数とする。

$$F_{i,j}(x',y') + \delta = g_{i,j} \pmod{\varepsilon} \qquad (9)$$

このとき、埋め込み強度εはユーザが自由に選択できるが、例えば、署名情報が1bitである時は、2以上の整数から選択する必要がある。そして、埋め込み済み画像の劣化を考え、小さな値とすることが望ましい。また、(x'、y')は、数論変換には変換領域に物理的意味がないという理由から、以下のランダム

関数により決定する。

まず、処理部1は、ランダム化関数$r_{x'}$、$r_{y'}$を記憶部5から参照して、各ブロックでばらつきのある埋め込み位置(x'、y')を決定する(S107)。ランダム化関数$r_{x'}$、$r_{y'}$は、埋め込み位置(x'、y')を一意に決定できるような関数であり、例えば次式のように設定できる。

$$x' = r_{x'}(P, i, j, f_{i,l}(0,0)) \quad (10)$$

$$y' = r_{y'}(P, i, j, f_{i,l}(0,0)) \quad (11)$$

$$l = j - 1 \pmod{L} \quad (12)$$

なお、この例で、ランダム化関数が原画像ブロック$f_{i,l}$(0、0)を含む関数になっているのは、安全性を高めるためであるが、詳細は「5.(7)」で後述する。なお、$f_{i,l}$(0、0)が左隣ブロックの(0、0)要素である。また、埋め込み処理ではこの(0、0)要素には変更がないため、抽出処理でも同じ$r_{x'}$、$r_{y'}$を設定しておけば、これらのランダム化関数からは同じ値を得ることができる。なお、左隣に限らず右隣りか所定のブロックの要素を用いても良いし、変更のない適当な要素を用いても良い。

また、処理部1は、埋め込むための署名画像の画素値$g_{i,j}$を記憶部5の署名画像ファイル53から読み込む(S109)。なお、ここではステップS107とステップS109を並列に処理しているが、ステップS107を処理した後に、ステップS109を処理しても良いし、ステップS109を処理した後に、ステップS107の処理を行うようにしても良い。

つぎに、処理部1は、求めた$F_{i,j}$(x'、y')及び$g_{i,j}$を用いて、上述の式(9)に基づいて、δを計算する(S111)。処理部1は、原画像ブロックの数論変換$F_{i,j}$(x、y)及びステップS111で求められたδを用いて、式(8)に従い、埋め込み済み画像ブロックの数論変換$H_{i,j}$(x、y)を計算する(S113)。さらに、処理部1は、上述の式(1)、(2)を用いて、$H_{i,j}$(x、y)の逆数論変換である埋め込み

画像ブロック$h_{i,j}(x,y)$を計算する(S115)。

図8に、埋め込みによる画素値への影響についての説明図を示す。

すなわち、$H_{i,j}(x,y)$の逆変換系列を$h_{i,j}(x,y)$とすると、数論変換の性質により図のように、

$$h_{x,y}(i,j) = \begin{cases} f_{x,y}(i,j) + \delta & i,j = N/2 \\ f_{x,y}(i,j) & \text{otherwise} \end{cases} \quad (13)$$

となる。Nが奇数の場合はこの関係は成立しないため、本実施の形態ではNは2以上の偶数から選択する必要がある。

処理部1は、求めた埋め込み済み画像ブロック$h_{i,j}(x,y)$を記憶部5の適宜のエリア(ワークエリア等)に記憶する(S117)。処理部 1 は、すべての(又は所望の範囲の)ブロックに対して上述の各ステップS101～S117処理を行った場合はステップS121に進み、そうでない場合はステップS103に戻り処理をやり直す(S119)。処理部1は、以上の処理をすべての(又は所望の範囲の)ブロックについて実行し、埋め込み済み画像[h]を得る。処理部1は、数論変換パラメータPと埋め込み済み画像[h]を埋め込み済み画像ファイル54に保存する(S121)。処理部1は、I/F6又は出力部3を介して、受信側装置にパラメータPと埋め込み済み画像[h]を送信する(S123)。処理部1は、必要に応じてパラメータとしてNを送るようにしても良い。なお、ここではステップS121とステップS123を並列して処理しているが、ステップS121を処理した後に、ステップS123を処理しても良いし、ステップS123を処理した後にステップS121の処理を行うようにしても良い。また、処理部1は、認証機関用装置(認証機関用コンピュータ30)に、法Pを、また、必要に応じて位数Nを送信するようにしてもよい。

3.2.2. 抽出処理

図9に、抽出処理のフローチャートを示す。

抽出処理が開始されると、処理部1は、数論変換のパラメータPと埋め込み済み画像[h]を送信側装置から受信し、埋め込み済み画像ファイル54に記憶する。また、処理部1は、場合によっては送信側装置から、さらにNを受信してもよい。また、処理部1は、数論変換のためのパラメータである法P、必要に応じてNを、認証機関装置から受信するようにしてもよい。なお、[h]が予め埋め込み済み画像ファイル54に記憶されている場合、ステップS201は省略することができる。処理部1は、埋め込み済み画像ファイル54を参照して、埋め込み済み画像[h]をブロック分割した埋め込み済み画像ブロック$h_{i,j}(x, y)$を読み込む(S203)。

つぎに、処理部1は、上述のステップS101と同様に、数論変換のためのパラメータP、N、αを設定する(S204)。処理部1は、設定されたパラメータを用い、式(1)、(2)に基づいて埋め込み済み画像ブロック$h_{i,j}(x, y)$を数論変換して$H_{i,j}(x, y)$を計算する(S205)。また、処理部1は、前述した署名画像の埋め込み済み位置に対応した署名画像抽出位置(x', y')を予め記憶部5に記憶されたランダム化関数$r_{x'}$、$r_{y'}$を用いて決定する(S207)。

つぎに、処理部1は、抽出位置の埋め込み済み画像ブロックの数論変換$H_{i,j}(x', y')$より署名画像の画素値$g_{i,j}$を抽出する(S209)。すなわち、処理部1は、次式のように、$H_{i,j}(x', y')$のεによる剰余を取ることによって署名画像の画素値を求める。なお、式(9)を変形すると、式(14)となり、署名画像の画素値$g_{i,j}$が抽出できる。

$$g_{i,j} = H_{i,j}(x', y') \pmod{\varepsilon} \qquad (14)$$

処理部1は、署名画像の画素値$g_{i,j}$を記憶部5の適宜のエリア(ワークエリア等)に記憶する(S211)。処理部1は、すべての(又は所定の範囲の)ブロックに対して処理ステップS201～S211を行った場合はステップS215に進み、

そうでない場合はステップS203に戻り上述の処理を繰り返す(S213)。処理部1は、以上の全ての(又は所定の範囲の)ブロックより$g_{i,j}$を抽出して、署名画像[g]を得る。処理部1は、署名画像[g]を記憶部5の署名画像ファイル53に保存し、表示部4に表示又は出力部3やインターフェース6から出力する(S215)。さらに、処理部1は、埋め込み済み画像[h]及び署名画像[g]に基づいて、原画像[f]を求め、適宜記憶及び/又は出力・表示するようにしてもよい。

ここで、PとNが正規の値であり、埋め込み済み画像[h]に改ざんがなければ正規の署名画像が取り出せる。一方、PとNが不正なものであるか、[h]に改ざんがある場合、改ざんされた場合の$H_{i,j}(x,y)$は数論変換の性質より正規の値と大きく異なる。ゆえに、それから抽出された署名情報は不正な値となる可能性が高い。よって、抽出された署名情報より構成された署名画像により、改ざんの有無とその位置を視認することができる。

4. 実験結果

図10に、実験に使用する画像の図を示す。図(a)は、現画像、図(b)は署名画像をそれぞれ示す。図(a)のようなSIDBAの標準画像であるText(256×256画素、8bit階調)に対して本発明を適用し、有効性について検討した。鍵となる数論変換のパラメータはP=85、147、693、N=4を用い、署名画像は図(b)(64×64画素、1bit階調)を用いた。また、埋め込み強度εは5を用いた。ランダム化関数$r_{x'}$、$r_{y'}$には最も簡単な例として、次式を用いた。

$$r_{x'} = 1 \times \{P + i + j + f_{i,l}(0,0)\} \pmod N$$

$$r_{y'} = 2 \times \{P + i + j + f_{i,l}(0,0)\} \pmod N$$

図11に、実験結果の画像の図(1)を示す。図(a)は、埋め込み済み画像、図(b)は抽出された署名画像をそれぞれ示す。図10(a)に対して埋め込み処

理を行った結果が図11(a)である。SNRは56．73dBとなり、埋め込みによる劣化はほとんど目立たなかった。

図12に、出力画像の画質と埋め込み強度εの関係について示す。

この図はεを2から12まで変化させ埋め込み処理を行った場合の、埋め込み済み画像のSNRとεの関係を示すグラフである。εの増加につれSNRが低下するのは、埋め込み処理におけるのδ値の大きさがεに比例するからである。いずれのεでも高い値を示したことから、劣化が目立たない画像であるといえる。また、図11(a)から抽出した署名画像が図11(b)であり、図10(b)と全く同じであった。

図13に、実験結果の画像の図(2)を示す。図(a)は、改ざん例の画像、図(b)は(a)から抽出された画像をそれぞれ示す。

この例では、図11(a)に対し、図13(a)のような改ざんを行った。改ざん例は、フォトレタッチソフトを使用して「0」の部分を含む矩形領域をコピーし、「8」の部分に張り付けたものである。図13(a)から抽出した署名画像が図13(b)である。改ざん箇所と署名画像が破壊されている部分が一致しており、改ざん位置が視認できることがわかった。

5．安全性についての議論

本発明の、埋め込み済み画像に改ざんが行われた場合への安全性について以下のように議論する。ただし攻撃者は埋め込み済み画像[h]とすべてのアルゴリズムが既知であり、鍵情報P、N、原画像[f]、署名画像[g]は未知であると仮定する。

(1)アルゴリズムから適切な改ざんを解析

ここでは簡単のため、N＝2の場合について議論する。a、b、c、dは正の整数として、

$$f_{i,j}(x,y) = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

とする。埋め込み処理により

$$h_{i,j}(x,y) = \begin{pmatrix} a & b \\ c & d+\delta \end{pmatrix}$$

となる。抽出処理においては数論変換により

$$H_{i,j}(x,y) = \begin{pmatrix} A+\delta & B-\delta \\ C-\delta & D+\delta \end{pmatrix}$$

を得て、式(14)により、正規の署名情報を得ることができる。

ここで、$h_{i,j}(x,y)$に

$$h_{i,j}(x,y) = \begin{pmatrix} a+\mu_1 & b+\mu_2 \\ c+\mu_3 & d+\delta+\mu_4 \end{pmatrix}$$

と改ざんが行われた場合を考える。ここで、μ_1、μ_2、μ_3、μ_4は整数とする。

抽出処理において、$h_{i,j}(x,y)$を数論変換すると

$$H_{i,j}(x,y) = \begin{pmatrix} A+\delta+\nu_1 & B-\delta+\nu_2 \\ C-\delta+\nu_3 & D+\delta+\nu_4 \end{pmatrix}$$

$$\nu_1 = \mu_1 + \mu_2 + \mu_3 + \mu_4$$

$$\nu_2 = \mu_1 + \mu_3 + \alpha(\mu_2 + \mu_4)$$

$$\nu_3 = \mu_1 + \mu_2 + \alpha(\mu_3 + \mu_4)$$

$$\nu_4 = \mu_1 + \alpha(\mu_2 + \mu_3) + \alpha^2\mu_4$$

となる。よってλ_1、λ_2、λ_3、λ_4を任意の正の整数とすると、

$$\nu_1 = \mu_1 + \mu_2 + \mu_3 + \mu_4 = \lambda_1\varepsilon$$

$$\nu_2 = \mu_1 + \mu_3 + \alpha(\mu_2 + \mu_4) = \lambda_2\varepsilon$$

$$\nu_3 = \mu_1 + \mu_2 + \alpha(\mu_3 + \mu_4) = \lambda_3\varepsilon$$

$$\nu_4 = \mu_1 + \alpha(\mu_2 + \mu_3) + \alpha^2\mu_4 = \lambda_4\varepsilon$$

を同時に満たすようなμ_1、μ_2、μ_3、μ_4であれば、本発明では改ざんを検出できない。これは、改ざんによってν_1、ν_2、ν_3、ν_4のeによる剰余が0になるからである。このときμ_1、μ_2、μ_3、μ_4についての連立方程式はαを含むものとなる。攻撃者はαが未知という仮定ではこの連立方程式は解析的に解くことは困難である。

(2)任意の部分的な改ざん

本発明において、署名情報は$H_{i,j}(x', y')$のεによる剰余により抽出する。これは、任意に改ざんを行ったとしても一つのブロックにつきε^{-1}の確率で正規の署名情報を得られることを意味する。一般に、画像の冗長性から一つのブロックのみを改ざんすることはほとんど意味をなさず、複数のブロックを改ざんする必要が生じる。T個のブロックを改ざんした場合、その改ざんが成功する確率はε^{-T}である。例えばN=2、ε=5である場合に、4×4ブロック(=8×

8画素）の改ざんに成功する確率は5^{-16}となり、この方法による改ざんは高い確率で検出できるといえる。ここで、εが大きいほど改ざんが難しくなるが、画像の劣化も大きくなるため、本発明では安全性と画像の品質はいわゆるトレードオフの関係にある。しかしながら、実験ではε＝12においてもSNRは48．2dBであり、εが比較的大きな値でも劣化の目立たない埋め込みが可能である。

（3）ビットプレーンへの改ざん

本発明はビットプレーンに基づいた埋め込み手法ではないため、それに注目した攻撃は意味をなさない。例えば、LSBのみへの改ざんは$h_{i,j}(x、y)$に対しては小さな影響しか与えないが、数論変換の性質から$H_{i,j}(x、y)$には大きな影響を与えるため、得られる署名情報は不正なものになる可能性が高い。

（4）鍵の全数探索

鍵であるPの全数探索では、Pは素数のべき乗による任意の合成数を選択することができるため、探索範囲は計算機上で扱える整数である。一方、Pが正しいかどうかについての判定は、抽出された署名画像が意味のあるものかどうかを人間が視認して行うが、これには多大な時間を要すると考えられる。ゆえに、鍵の全数探索は現実的に困難である。

（5）拡大縮小、回転などの幾何学的な変化

本発明では解像度や形状の変化がある場合には、$r_{x'}$、$r_{y'}$やNの対応がとれないために画像全体の改ざんとして検出される。

（6）同じ画像内の切り張り

[h]をブロック分割し、それらの位置を交換したり、ブロックをコピーし任意の場所に張り付ける改ざんを考える。実験における改ざんはこれに当たる。この場合、本発明での$r_{x'}$、$r_{y'}$はi、jを含む関数であるため、この方法の改ざんでは位置を移動したブロックでは$r_{x'}$、$r_{y'}$の対応が正しく取れない。よって、この方法による改ざんは高い確率で検出できる。

(7)埋め込み処理された複数の異なる画像間で切り張り

例えば、異なる複数の埋め込み済み画像をそれぞれブロック分割し、同じ位置にあるブロックを入れ替えることで一つの画像を合成する場合を考える。ただし、これらの画像の解像度はすべて等しく、埋め込み処理におけるP、N、[g]がすべて同じであるとする。この場合、本発明では$r_{x'}$、$r_{y'}$は左隣ブロックの画素値である$f_{i,j}(0,0)$を含む関数で生成しているため、$r_{x'}$、$r_{y'}$の正しい対応が取れない。よって、この方法による改ざんは高い確率で検出できる。

6. むすび

本発明では、従来の直交変換を用いた耐性型電子透かしの応用として、数論変換による脆弱型電子透かしによる改ざん位置検出について提案した。実験では提案法の有効性について検討し、良好な結果を得た。また、様々な攻撃に対する提案法の安全性についての考察を行った。

本発明の改ざん検出方法又は改ざん検出装置・システムは、その各手順をコンピュータに実行させるための改ざん検出プログラム、改ざん検出プログラムを記録したコンピュータ読み取り可能な記録媒体、改ざん検出プログラムを含みコンピュータの内部メモリにロード可能なプログラム製品、そのプログラムを含むサーバ等のコンピュータ、等により提供されることができる。

さらに、応用範囲として、本発明の改ざん検出方法の機能又は改ざん検出プログラムとその実行機能を、ディジタルカメラやスキャナ等の各種画像入力装置に搭載し、そのような装置から取り込んだ画像に透かし情報を埋め込むようにすることもできる。

産業上の利用可能性

本発明によると、以上のように、直交変換を用いた耐性型電子透かし法を応用した数論変換による脆弱型の電子透かし法を用いた改ざん検出方法、改ざん検出プログラム及びそのプログラムを記録した記録媒体を提案することがで

きる。また、本発明によると、改ざんの有無及びその位置を目視によって容易に確認することができる改ざん検出法等を提供することができる。

さらに、従来の数論変換を利用した電子透かしの手法では、原画像の画像ビットを下位2bit程度という比較的少ない範囲で置換することにより署名情報を埋め込むものであった。これに対して、本発明では、原画像の画素ビットの全て又は所望の広範囲を利用して署名情報を埋め込むことにより安全性を一層高めることができる。また、従来の数論変換を利用した手法では、署名情報の埋め込みを数論変換ドメインに掛け合わせて(畳み込んで)実現していた。これに対して、本発明では、署名情報の埋め込みを足し算により実現することで、数値誤差を小さくし、演算速度を速くすることができる。

請 求 の 範 囲

1. 処理部は、数論変換のパラメータである法P、位数N、根αを設定するステップと、

処理部は、記憶部から、埋め込み対象の原画像[f]をブロック分割した原画像ブロック$f_{i,j}(x,y)$を読み込むステップと、

処理部は、設定された法P、位数N、根αを用いて、原画像ブロック$f_{i,j}(x,y)$を数論変換して原画像ブロックの数論変換ブロック$F_{i,j}(x,y)$を計算するステップと、

処理部は、各ブロックにおける署名画像の埋め込み位置(x'、y')を、所定のランダム化関数に基づき決定するステップと、

処理部は、埋め込むための署名画像の画素値$g_{i,j}$を記憶部から読み込むステップと、

処理部は、埋め込み位置の原画像ブロックの数論変換ブロック$F_{i,j}(x',y')$と署名画像の画素値$g_{i,j}$と埋め込み強度εより、各ブロックの埋め込み量δを求めるステップと、

処理部は、原画像ブロックの数論変換ブロック$F_{i,j}(x,y)$に、(x、y)に応じて埋め込み量δを加算又は減算して、埋め込み済み画像ブロックの数論変換ブロック$H_{i,j}(x,y)$を求めるステップと、

処理部は、数論変換ブロック$H_{i,j}(x,y)$の逆数論変換を計算して、埋め込み済み画像ブロック$h_{i,j}(x,y)$を求めるステップと、

処理部は、全ての又は所望の範囲の(i, j)ブロックについて埋め込み済み画像ブロック$h_{i,j}(x,y)$を求めることにより埋め込み済み画像[h]を得て、それを記憶部に記憶する、及び／又は、出力部若しくはインターフェースにより出力するステップと

を含む改ざん検出方法。

2. 処理部は、埋め込み済み画像[h]をブロック分割した埋め込み済み画像

ブロック$h_{i,j}(x、y)$を、記憶部又は入力部又はインターフェースから読み込むステップと、

処理部は、数論変換のためのパラメータである法P、位数N、根αを設定するステップと、

処理部は、埋め込み済み画像ブロック$h_{i,j}(x、y)$を数論変換して埋め込み済み画像ブロックの数論変換ブロック$H_{i,j}(x、y)$を計算するステップと、

処理部は、署名画像の埋め込み位置に対応する抽出位置(x'、y')を所定のランダム化関数に基づいて決定するステップと、

処理部は、抽出位置の数論変換ブロック$H_{i,j}(x'、y')$の埋め込み強度εによる剰余を取ることによって、署名画像の画素値$g_{i,j}$を抽出するステップと、

処理部は、全ての又は所望の範囲の(i, j)ブロックについて署名画像の画素値$g_{i,j}$を求めることにより署名画像[g]を得て、それを記憶部に記憶する、及び／又は、表示部若しくは出力部若しくはインターフェースに出力するステップと

を含む改ざん検出方法。

3. 署名画像を原画像に埋め込む処理及び署名画像を抽出する処理を含む改ざん検出方法であって、

前記埋め込む処理は、

処理部は、数論変換のパラメータである法P、位数N、根αを設定するステップと、

処理部は、記憶部から、埋め込み対象の原画像[f]をブロック分割した原画像ブロック$f_{i,j}(x、y)$を読み込むステップと、

処理部は、設定された法P、位数N、根αを用いて、原画像ブロック$f_{i,j}(x、y)$を数論変換して原画像ブロックの数論変換ブロック$F_{i,j}(x、y)$を計算するステップと、

処理部は、各ブロックにおける署名画像の埋め込み位置(x'、y')を、所

定のランダム化関数に基づき決定するステップと、

処理部は、埋め込むための署名画像の画素値$g_{i,j}$を記憶部から読み込むステップと、

処理部は、埋め込み位置の原画像ブロックの数論変換ブロック$F_{i,j}(x', y')$と署名画像の画素値$g_{i,j}$と埋め込み強度εにより、各ブロックの埋め込み量δを求めるステップと、

処理部は、原画像ブロックの数論変換ブロック$F_{i,j}(x, y)$に、(x、y)に応じて埋め込み量δを加算又は減算して、埋め込み済み画像ブロックの数論変換ブロック$H_{i,j}(x, y)$を求めるステップと、

処理部は、数論変換ブロック$H_{i,j}(x, y)$の逆数論変換を計算して、埋め込み済み画像ブロック$h_{i,j}(x, y)$を求めるステップと、

処理部は、全ての又は所望の範囲の(i, j)ブロックについて埋め込み済み画像ブロック$h_{i,j}(x, y)$を求めることにより埋め込み済み画像[h]を得て、それを記憶部に記憶する、及び／又は、出力部若しくはインターフェースにより出力するステップと

を含み、

前記抽出処理は、

処理部は、埋め込み済み画像[h]をブロック分割した埋め込み済み画像ブロック$h_{i,j}(x, y)$を、記憶部又は入力部又はインターフェースから読み込むステップと、

処理部は、数論変換のためのパラメータである法P、位数N、根αを設定するステップと、

処理部は、埋め込み済み画像ブロック$h_{i,j}(x, y)$を数論変換して埋め込み済み画像ブロックの数論変換ブロック$H_{i,j}(x, y)$を計算するステップと、

処理部は、署名画像の埋め込み位置に対応する抽出位置(x'、y')を所定のランダム化関数に基づいて決定するステップと、

処理部は、抽出位置の数論変換ブロック$H_{i,j}(x', y')$の埋め込み強度εによる剰余を取ることによって、署名画像の画素値$g_{i,j}$を抽出するステップ

と、

処理部は、全ての又は所望の範囲の(i, j)ブロックについて署名画像の画素値$g_{i,j}$を求めることにより署名画像[g]を得て、それを記憶部に記憶する、及び／又は、表示部若しくは出力部若しくはインターフェースに出力するステップと

を含む改ざん検出方法。

4. 処理部は、出力部又はインターフェースを介して、抽出側装置に、法P及び埋め込み済み画像[h]を、また、必要に応じて位数Nを送信するステップをさらに含む請求項1または3に記載の改ざん検出方法。

5. 処理部は、数論変換のためのパラメータである法Pと埋め込み済み画像[h]、必要に応じてNを送信側装置から受信するステップをさらに含む請求項2又は3に記載の改ざん検出方法。

6. 処理部は、埋め込み済み画像[h]及び署名画像[g]に基づいて、原画像[f]を求めるステップをさらに含む請求項1乃至3のいずれかに記載の改ざん検出方法。

7. Pは、素数のべき乗による任意の合成数であることを特徴とする請求項1乃至3のいずれかに記載の改ざん検出方法。

8. Nは、署名画像の埋め込み側及び抽出側で共通にあらかじめ記憶部に記憶してあること、又は、埋め込み側から抽出側へ伝送されることを特徴とする請求項1乃至3のいずれかに記載の改ざん検出方法。

9. 処理部は、$N \mid GCD[(p_1-1),(p_2-1),\cdots,(p_m-1)]$ により求められた位数Nの候補から、予め定められた優先順位でいずれかの位数Nを選択することを特徴とする請求項1乃至3のいずれかに記載の改ざん検出方

法。

10. 処理部は、設定された法P及び位数Nに基づき、一意に算出される中国剰余定理等の予め定められた式により根αを計算することを特徴とする請求項1乃至3のいずれかに記載の改ざん検出方法。

11. 処理部は、p_iを素数、r_iを正の整数として、$P=p_1^{r1}p_2^{r2}\cdots p_m^{rm}$ で表されるとしたPを設定し、

処理部は、位数Nを、$N \mid GCD[(p_1-1),(p_2-1),\cdots,(p_m-1)]$ を満たす正の整数から選択し、又は、記憶部から読み取り、

処理部は、p_iを法とする位数Nの根$\alpha_{1,i}$を計算し、

処理部は、p_i^{ri}を法とする位数Nの根$\alpha_{2,i}$を、$\alpha_{1,i}$より求め、

処理部は、中国剰余定理により、Pを法とする位数Nの根αを、$\alpha_{2,i}$より求める

ことを特徴とする請求項1乃至3のいずれかに記載の改ざん検出方法。

12. 処理部は、P、N及びαを用いて、次式によりx(n)とX(k)との間の数論変換を実行することを特徴とする請求項1乃至3のいずれかに記載の改ざん検出方法。

$$X(k)=\sum_{n=0}^{N-1}x(n)\alpha^{kn} \pmod P \qquad (1)$$

$$x(n)=N^{-1}\sum_{k=0}^{N-1}X(k)\alpha^{-kn} \pmod P \qquad (2)$$

(ここに、P(素数のべき乗となる任意の合成数)、α、(を正の整数、Nを$\alpha^N=1 \pmod P$となる最小の正の整数)

$X=[T]x$

$x=[T]^{-1}X$

([T]:変換行列、$[T]^{-1}$:逆変換行列)

13. 前記ランダム化関数は、法Pの値、及び／又は、隣接するブロック若しくは埋め込み処理で変更されない所定ブロックの画素値をパラメータとし、位置を一意に決定する関数であることを特徴とする請求項1乃至3のいずれかに記載の改ざん検出方法。

14. 前記ランダム化関数は、以下の式による関数であることを特徴とする請求項1乃至3のいずれかに記載の改ざん検出方法。

$$x' = r_{x'}(P, i, j, f_{i,l}(0,0)) \quad (10)$$

$$y' = r_{y'}(P, i, j, f_{i,l}(0,0)) \quad (11)$$

$$l = j - 1 \pmod{L} \quad (12)$$

15. 処理部は、数論変換のパラメータである法P、位数N、根αを設定するステップと、

処理部は、記憶部から、埋め込み対象の原画像[f]をブロック分割した原画像ブロック$f_{i,j}(x,y)$を読み込むステップと、

処理部は、設定された法P、位数N、根αを用いて、原画像ブロック$f_{i,j}(x,y)$を数論変換して原画像ブロックの数論変換ブロック$F_{i,j}(x,y)$を計算するステップと、

処理部は、各ブロックにおける署名画像の埋め込み位置(x'、y')を、所定のランダム化関数に基づき決定するステップと、

処理部は、埋め込むための署名画像の画素値$g_{i,j}$を記憶部から読み込むステップと、

処理部は、埋め込み位置の原画像ブロックの数論変換ブロック$F_{i,j}(x', y')$と署名画像の画素値$g_{i,j}$と埋め込み強度εにより、各ブロックの埋め込み量δを求めるステップと、

処理部は、原画像ブロックの数論変換ブロック$F_{i,j}(x,y)$に、(x、y)に応じ

て埋め込み量δを加算又は減算して、埋め込み済み画像ブロックの数論変換ブロック$H_{i,j}(x, y)$を求めるステップと、

処理部は、数論変換ブロック$H_{i,j}(x, y)$の逆数論変換を計算して、埋め込み済み画像ブロック$h_{i,j}(x, y)$を求めるステップと、

処理部は、全ての又は所望の範囲の(i, j)ブロックについて埋め込み済み画像ブロック$h_{i,j}(x, y)$を求めることにより埋め込み済み画像[h]を得て、それを記憶部に記憶する、及び／又は、出力部若しくはインターフェースにより出力するステップと

をコンピュータに実行させるための改ざん検出プログラム。

16. 処理部は、埋め込み済み画像[h]をブロック分割した埋め込み済み画像ブロック$h_{i,j}(x, y)$を、記憶部又は入力部又はインターフェースから読み込むステップと、

処理部は、数論変換のためのパラメータである法P、位数N、根αを設定するステップと、

処理部は、埋め込み済み画像ブロック$h_{i,j}(x, y)$を数論変換して埋め込み済み画像ブロックの数論変換ブロック$H_{i,j}(x, y)$を計算するステップと、

処理部は、署名画像の埋め込み位置に対応する抽出位置(x'、y')を所定のランダム化関数に基づいて決定するステップと、

処理部は、抽出位置の数論変換ブロック$H_{i,j}(x', y')$の埋め込み強度εによる剰余を取ることによって、署名画像の画素値$g_{i,j}$を抽出するステップと、

処理部は、全ての又は所望の範囲の(i, j)ブロックについて署名画像の画素値$g_{i,j}$を求めることにより署名画像[g]を得て、それを記憶部に記憶する、及び／又は、表示部若しくは出力部若しくはインターフェースに出力するステップと

をコンピュータに実行させるための改ざん検出プログラム。

17. 署名画像を原画像に埋め込む処理及び署名画像を抽出する処理を含む改ざん検出方法であって、

前記埋め込む処理は、

処理部は、数論変換のパラメータである法P、位数N、根αを設定するステップと、

処理部は、記憶部から、埋め込み対象の原画像[f]をブロック分割した原画像ブロック$f_{i,j}(x,y)$を読み込むステップと、

処理部は、設定された法P、位数N、根αを用いて、原画像ブロック$f_{i,j}(x,y)$を数論変換して原画像ブロックの数論変換ブロック$F_{i,j}(x,y)$を計算するステップと、

処理部は、各ブロックにおける署名画像の埋め込み位置(x'、y')を、所定のランダム化関数に基づき決定するステップと、

処理部は、埋め込むための署名画像の画素値$g_{i,j}$を記憶部から読み込むステップと、

処理部は、埋め込み位置の原画像ブロックの数論変換ブロック$F_{i,j}(x',y')$と署名画像の画素値$g_{i,j}$と埋め込み強度εにより、各ブロックの埋め込み量δを求めるステップと、

処理部は、原画像ブロックの数論変換ブロック$F_{i,j}(x,y)$に、(x、y)に応じて埋め込み量δを加算又は減算して、埋め込み済み画像ブロックの数論変換ブロック$H_{i,j}(x,y)$を求めるステップと、

処理部は、数論変換ブロック$H_{i,j}(x,y)$の逆数論変換を計算して、埋め込み済み画像ブロック$h_{i,j}(x,y)$を求めるステップと、

処理部は、全ての又は所望の範囲の(i, j)ブロックについて埋め込み済み画像ブロック$h_{i,j}(x,y)$を求めることにより埋め込み済み画像[h]を得て、それを記憶部に記憶する、及び／又は、出力部若しくはインターフェースにより出力するステップと

を含み、

前記抽出処理は、

処理部は、埋め込み済み画像[h]をブロック分割した埋め込み済み画像

ブロック$h_{i,j}(x, y)$を、記憶部又は入力部又はインターフェースから読み込むステップと、

処理部は、数論変換のためのパラメータである法P、位数N、根αを設定するステップと、

処理部は、埋め込み済み画像ブロック$h_{i,j}(x, y)$を数論変換して埋め込み済み画像ブロックの数論変換ブロック$H_{i,j}(x, y)$を計算するステップと、

処理部は、署名画像の埋め込み位置に対応する抽出位置(x'、y')を所定のランダム化関数に基づいて決定するステップと、

処理部は、抽出位置の数論変換ブロック$H_{i,j}(x', y')$の埋め込み強度εによる剰余を取ることによって、署名画像の画素値$g_{i,j}$を抽出するステップと、

処理部は、全ての又は所望の範囲の(i, j)ブロックについて署名画像の画素値$g_{i,j}$を求めることにより署名画像[g]を得て、それを記憶部に記憶する、及び／又は、表示部若しくは出力部若しくはインターフェースに出力するステップと

をコンピュータに実行させるための改ざん検出プログラム。

18. 処理部は、数論変換のパラメータである法P、位数N、根αを設定するステップと、

処理部は、記憶部から、埋め込み対象の原画像[f]をブロック分割した原画像ブロック$f_{i,j}(x, y)$を読み込むステップと、

処理部は、設定された法P、位数N、根αを用いて、原画像ブロック$f_{i,j}(x, y)$を数論変換して原画像ブロックの数論変換ブロック$F_{i,j}(x, y)$を計算するステップと、

処理部は、各ブロックにおける署名画像の埋め込み位置(x'、y')を、所定のランダム化関数に基づき決定するステップと、

処理部は、埋め込むための署名画像の画素値$g_{i,j}$を記憶部から読み込むステップと、

処理部は、埋め込み位置の原画像ブロックの数論変換ブロック$F_{i,j}(x', y')$と署名画像の画素値$g_{i,j}$と埋め込み強度εにより、各ブロックの埋め込み量δを求めるステップと、

処理部は、原画像ブロックの数論変換ブロック$F_{i,j}(x, y)$に、(x、y)に応じて埋め込み量δを加算又は減算して、埋め込み済み画像ブロックの数論変換ブロック$H_{i,j}(x, y)$を求めるステップと、

処理部は、数論変換ブロック$H_{i,j}(x, y)$の逆数論変換を計算して、埋め込み済み画像ブロック$h_{i,j}(x, y)$を求めるステップと、

処理部は、全ての又は所望の範囲の(i, j)ブロックについて埋め込み済み画像ブロック$h_{i,j}(x, y)$を求めることにより埋め込み済み画像[h]を得て、それを記憶部に記憶する、及び／又は、出力部若しくはインターフェースにより出力するステップと

をコンピュータに実行させるための改ざん検出プログラムを記録した記録媒体。

19. 処理部は、埋め込み済み画像[h]をブロック分割した埋め込み済み画像ブロック$h_{i,j}(x, y)$を、記憶部又は入力部又はインターフェースから読み込むステップと、

処理部は、数論変換のためのパラメータである法P、位数N、根αを設定するステップと、

処理部は、埋め込み済み画像ブロック$h_{i,j}(x, y)$を数論変換して埋め込み済み画像ブロックの数論変換ブロック$H_{i,j}(x, y)$を計算するステップと、

処理部は、署名画像の埋め込み位置に対応する抽出位置(x'、y')を所定のランダム化関数に基づいて決定するステップと、

処理部は、抽出位置の数論変換ブロック$H_{i,j}(x', y')$の埋め込み強度εによる剰余を取ることによって、署名画像の画素値$g_{i,j}$を抽出するステップと、

処理部は、全ての又は所望の範囲の(i, j)ブロックについて署名画像の

画素値$g_{i,j}$を求めることにより署名画像[g]を得て、それを記憶部に記憶する、及び／又は、表示部若しくは出力部若しくはインターフェースに出力するステップと

をコンピュータに実行させるための改ざん検出プログラムを記録した記録媒体。

20. 署名画像を原画像に埋め込む処理及び署名画像を抽出する処理を含む改ざん検出方法であって、

前記埋め込む処理は、

処理部は、数論変換のパラメータである法P、位数N、根αを設定するステップと、

処理部は、記憶部から、埋め込み対象の原画像[f]をブロック分割した原画像ブロック$f_{i,j}(x,y)$を読み込むステップと、

処理部は、設定された法P、位数N、根αを用いて、原画像ブロック$f_{i,j}(x,y)$を数論変換して原画像ブロックの数論変換ブロック$F_{i,j}(x,y)$を計算するステップと、

処理部は、各ブロックにおける署名画像の埋め込み位置(x'、y')を、所定のランダム化関数に基づき決定するステップと、

処理部は、埋め込むための署名画像の画素値$g_{i,j}$を記憶部から読み込むステップと、

処理部は、埋め込み位置の原画像ブロックの数論変換ブロック$F_{i,j}(x',y')$と署名画像の画素値$g_{i,j}$と埋め込み強度εにより、各ブロックの埋め込み量δを求めるステップと、

処理部は、原画像ブロックの数論変換ブロック$F_{i,j}(x,y)$に、(x、y)に応じて埋め込み量δを加算又は減算して、埋め込み済み画像ブロックの数論変換ブロック$H_{i,j}(x,y)$を求めるステップと、

処理部は、数論変換ブロック$H_{i,j}(x,y)$の逆数論変換を計算して、埋め込み済み画像ブロック$h_{i,j}(x,y)$を求めるステップと、

処理部は、全ての又は所望の範囲の(i, j)ブロックについて埋め込み済み

画像ブロック$h_{i,j}(x,y)$を求めることにより埋め込み済み画像[h]を得て、それを記憶部に記憶する、及び／又は、出力部若しくはインターフェースにより出力するステップと

を含み、

前記抽出処理は、

処理部は、埋め込み済み画像[h]をブロック分割した埋め込み済み画像ブロック$h_{i,j}(x,y)$を、記憶部又は入力部又はインターフェースから読み込むステップと、

処理部は、数論変換のためのパラメータである法P、位数N、根αを設定するステップと、

処理部は、埋め込み済み画像ブロック$h_{i,j}(x,y)$を数論変換して埋め込み済み画像ブロックの数論変換ブロック$H_{i,j}(x,y)$を計算するステップと、

処理部は、署名画像の埋め込み位置に対応する抽出位置(x',y')を所定のランダム化関数に基づいて決定するステップと、

処理部は、抽出位置の数論変換ブロック$H_{i,j}(x',y')$の埋め込み強度εによる剰余を取ることによって、署名画像の画素値$g_{i,j}$を抽出するステップと、

処理部は、全ての又は所望の範囲の(i, j)ブロックについて署名画像の画素値$g_{i,j}$を求めることにより署名画像[g]を得て、それを記憶部に記憶する、及び／又は、表示部若しくは出力部若しくはインターフェースに出力するステップと

をコンピュータに実行させるための改ざん検出プログラムを記録した記録媒体。

素数 13 の y^x (mod 13) の表

y^x	1	2	3	4	5	6	7	8	9	10	11	12	位数
1	1	1	1	1	1	1	1	1	1	1	1	1	1
2	2	4	8	3	6	12	11	9	5	10	7	1	12
3	3	9	1	3	9	1	3	9	1	3	9	1	3
4	4	3	12	9	10	1	4	3	12	9	10	1	6
5	5	12	8	1	5	12	8	1	5	12	8	1	4
6	6	10	8	9	2	12	7	3	5	4	11	1	12
7	7	10	5	9	11	12	6	3	8	4	2	1	12
8	8	12	5	1	8	12	5	1	8	12	5	1	4
9	9	3	1	9	3	1	9	3	1	9	3	1	3
10	10	9	12	3	4	1	10	9	12	3	4	1	6
11	11	4	5	3	7	12	2	9	8	10	6	1	12
12	12	1	12	1	12	1	12	1	12	1	12	1	2

図 1

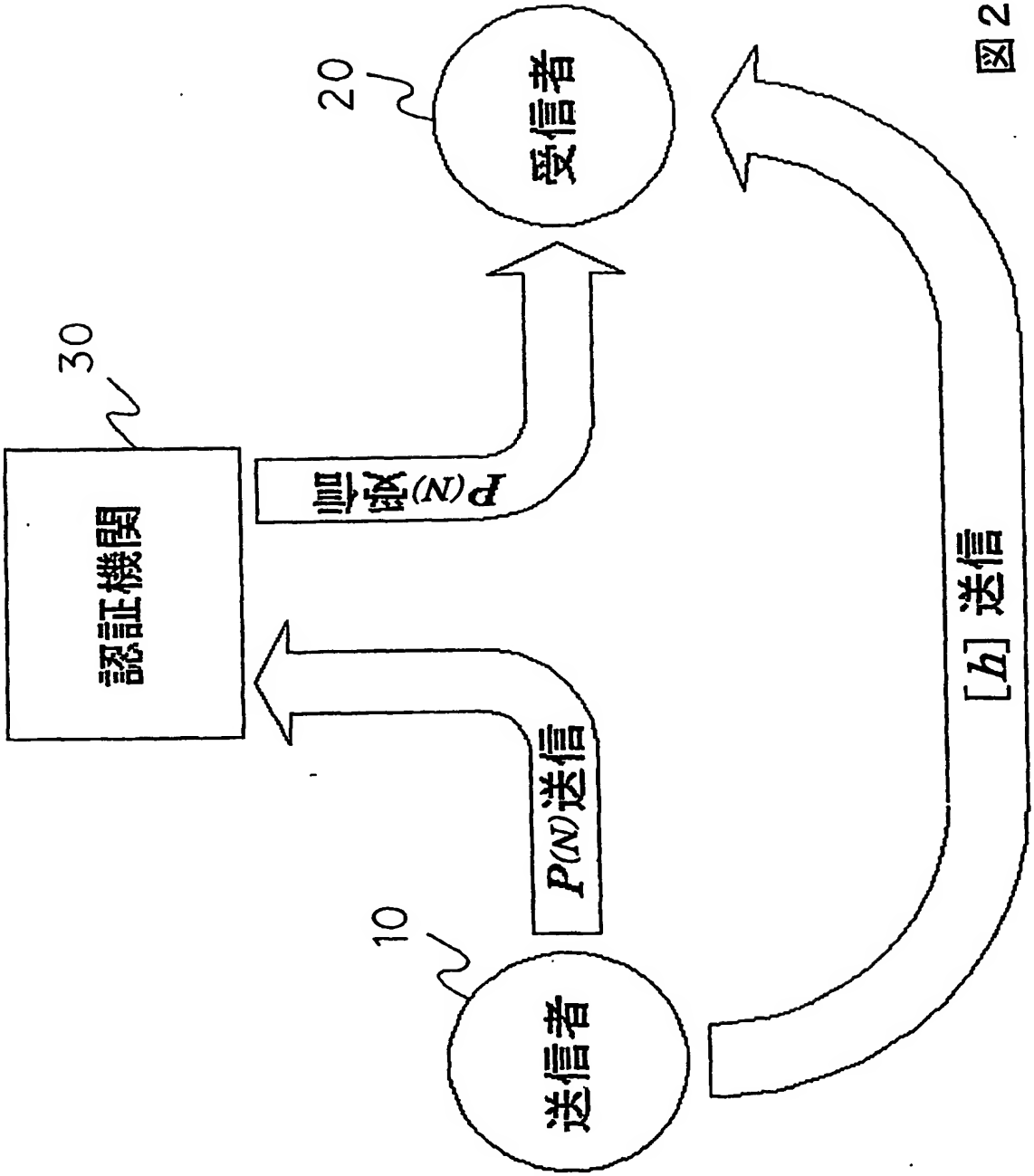


図2

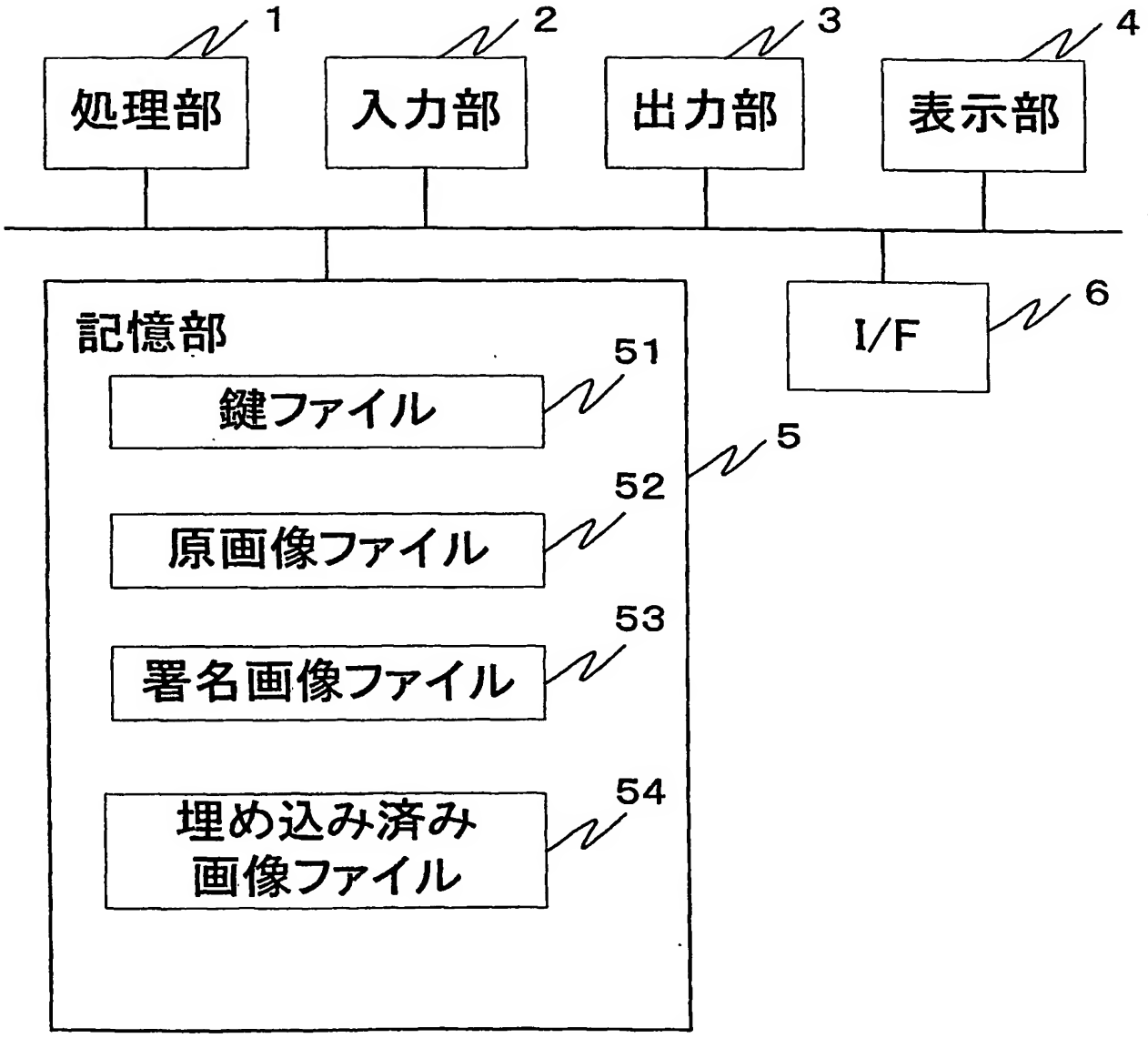

1
処理部
2
入力部
3
出力部
4
表示部
記憶部
51
鍵ファイル
52
原画像ファイル
53
署名画像ファイル
54
埋め込み済み
画像ファイル
5
I/F
6

図３

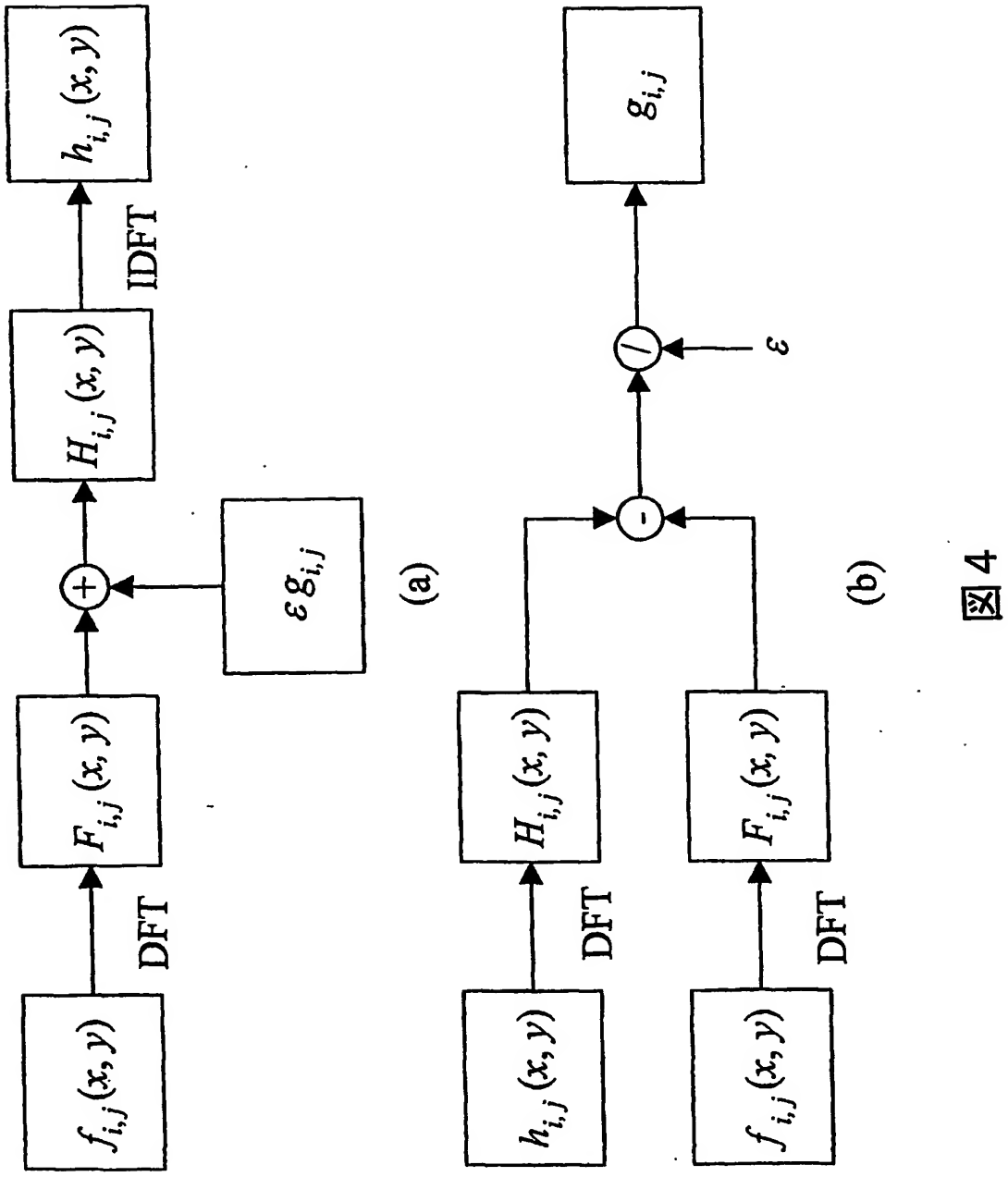

$f_{i,j}(x,y)$
DFT
$F_{i,j}(x,y)$
$\varepsilon g_{i,j}$
$H_{i,j}(x,y)$
IDFT
$h_{i,j}(x,y)$
(a)
$h_{i,j}(x,y)$
DFT
$H_{i,j}(x,y)$
$f_{i,j}(x,y)$
DFT
$F_{i,j}(x,y)$
ε
$g_{i,j}$
(b)

図4

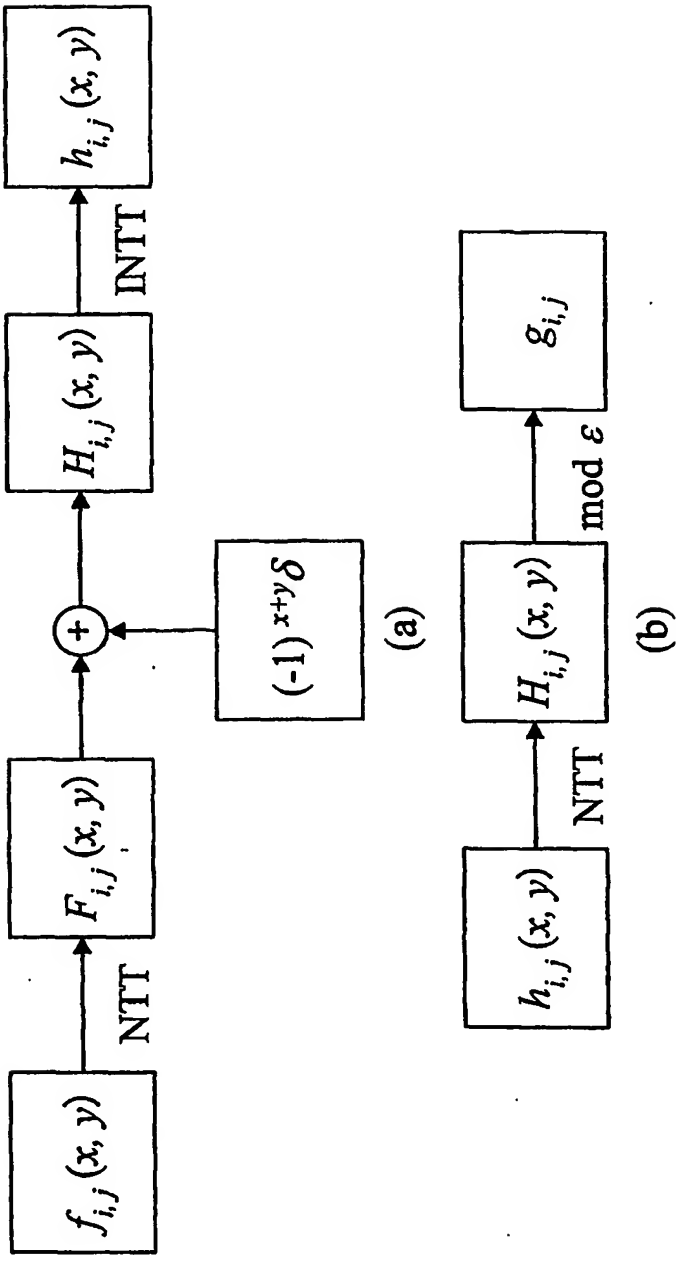

$f_{i,j}(x, y)$
NTT
$F_{i,j}(x, y)$
$(-1)^{x+y}\delta$
$H_{i,j}(x, y)$
NTT
$h_{i,j}(x, y)$
(a)
$h_{i,j}(x, y)$
NTT
$H_{i,j}(x, y)$
mod ε
$g_{i,j}$
(b)

図5

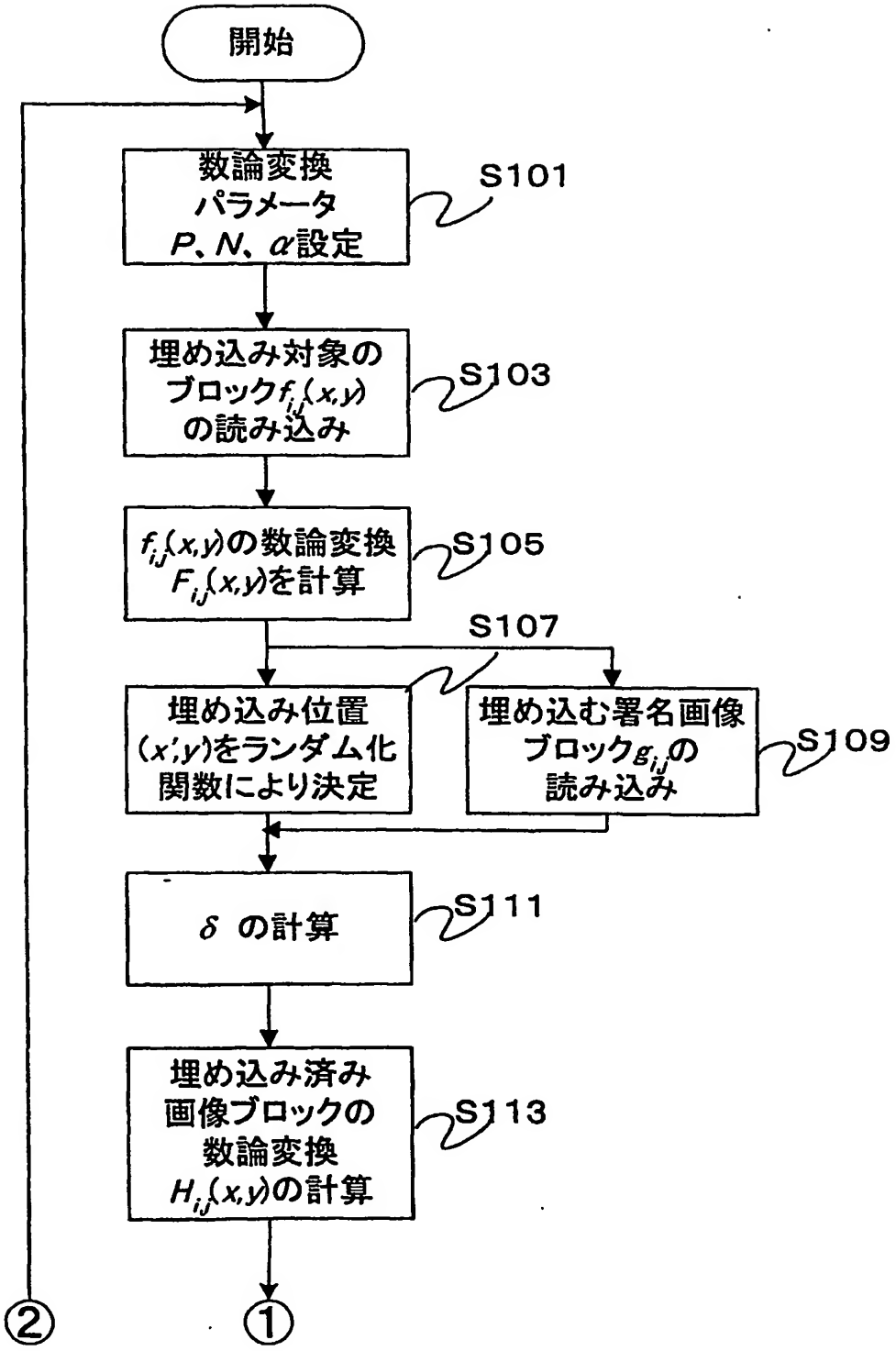

開始
数論変換
パラメータ
P、N、α設定
S101
埋め込み対象の
ブロック$f_{ij}(x,y)$
の読み込み
S103
$f_{ij}(x,y)$の数論変換
$F_{ij}(x,y)$を計算
S105
S107
埋め込み位置
(x',y')をランダム化
関数により決定
埋め込む署名画像
ブロックg_{ij}の
読み込み
S109
δ の計算
S111
埋め込み済み
画像ブロックの
数論変換
$H_{ij}(x,y)$の計算
S113
②
①

図6

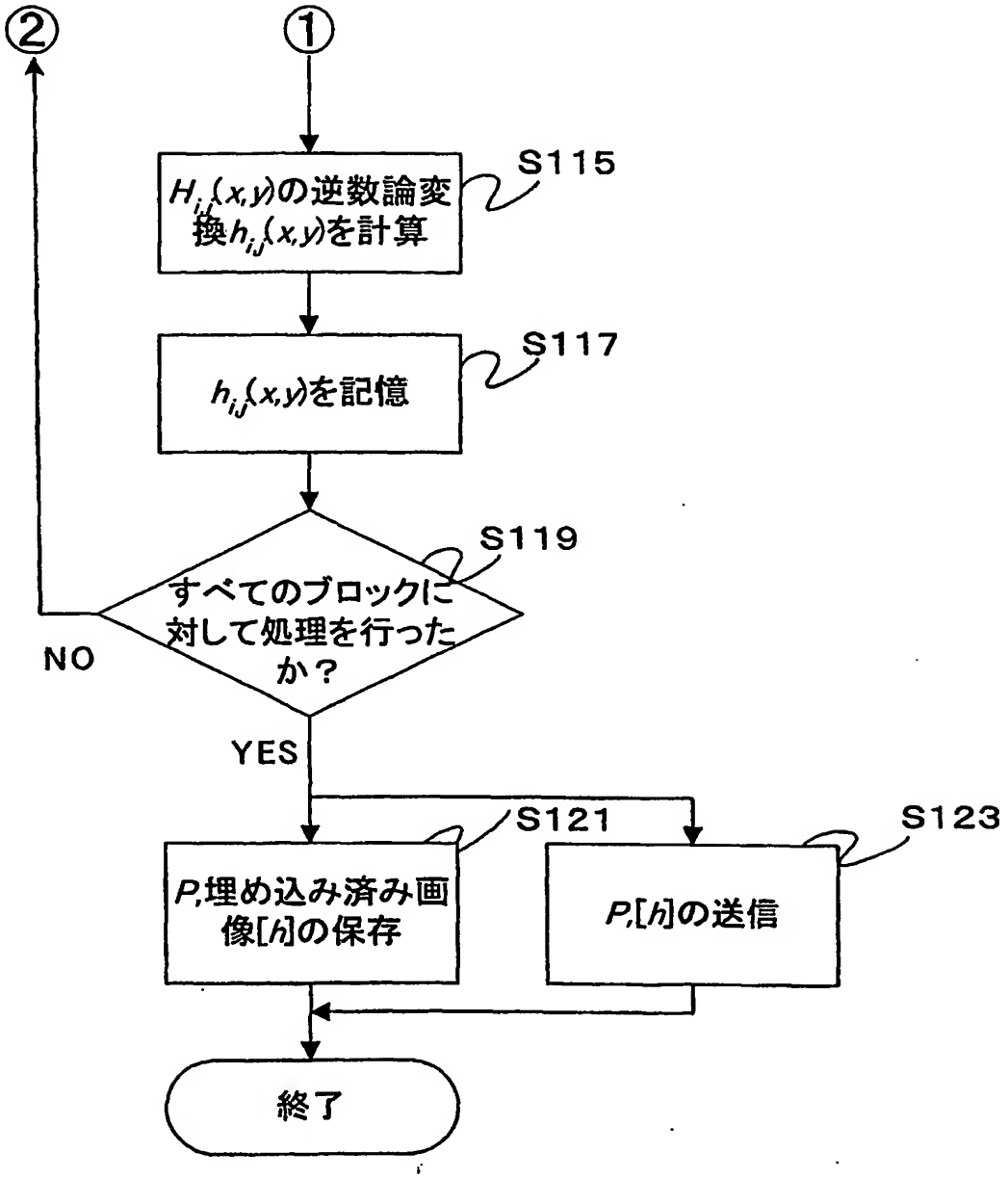

②
①
$H_{i,j}(x,y)$の逆数論変換$h_{i,j}(x,y)$を計算
S115
$h_{i,j}(x,y)$を記憶
S117
すべてのブロックに対して処理を行ったか？
S119
NO
YES
P_i埋め込み済み画像[h]の保存
S121
P_i[h]の送信
S123
終了

図7

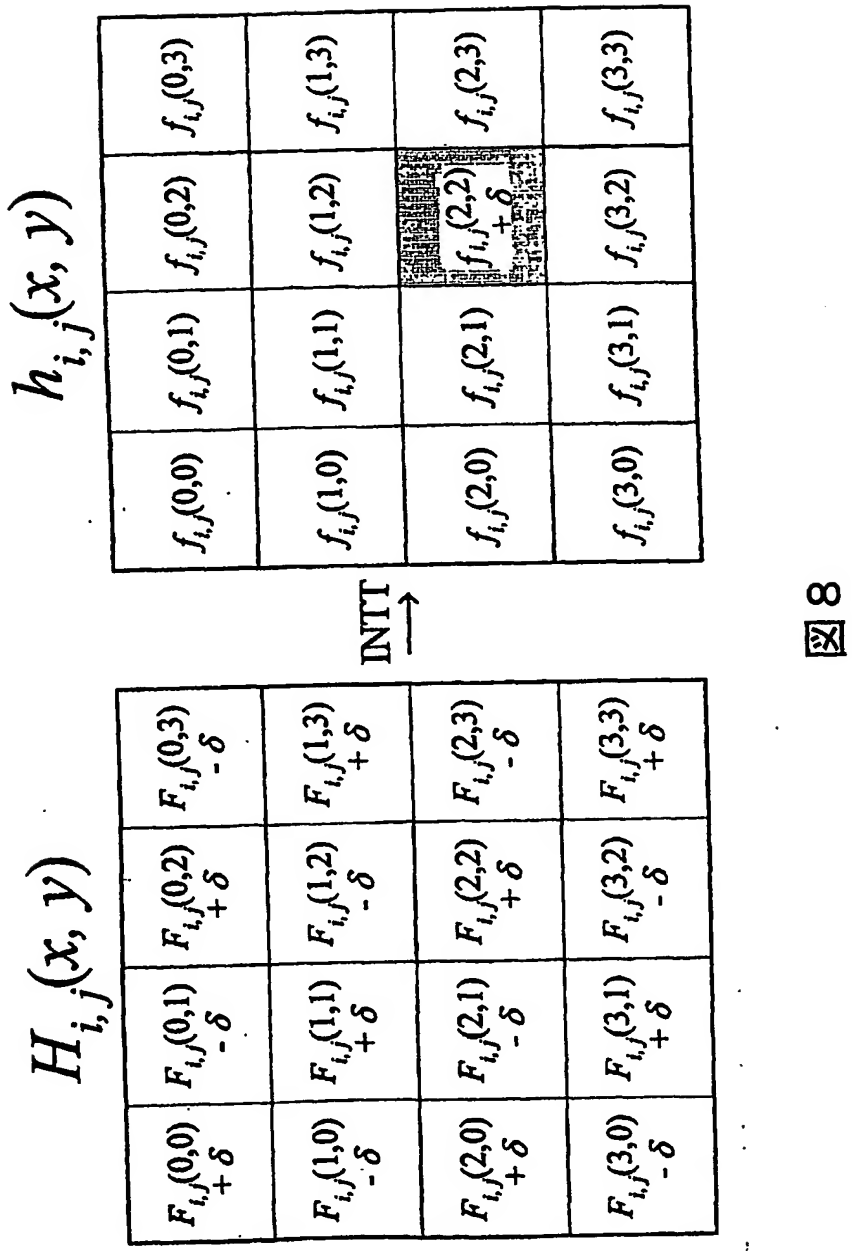

$h_{i,j}(x, y)$
$f_{i,j}(0,0)$ $f_{i,j}(0,1)$ $f_{i,j}(0,2)$ $f_{i,j}(0,3)$
$f_{i,j}(1,0)$ $f_{i,j}(1,1)$ $f_{i,j}(1,2)$ $f_{i,j}(1,3)$
$f_{i,j}(2,0)$ $f_{i,j}(2,1)$ $f_{i,j}(2,2)+\delta$ $f_{i,j}(2,3)$
$f_{i,j}(3,0)$ $f_{i,j}(3,1)$ $f_{i,j}(3,2)$ $f_{i,j}(3,3)$
INTT
$H_{i,j}(x, y)$
$F_{i,j}(0,0)+\delta$ $F_{i,j}(0,1)-\delta$ $F_{i,j}(0,2)+\delta$ $F_{i,j}(0,3)-\delta$
$F_{i,j}(1,0)-\delta$ $F_{i,j}(1,1)+\delta$ $F_{i,j}(1,2)-\delta$ $F_{i,j}(1,3)+\delta$
$F_{i,j}(2,0)+\delta$ $F_{i,j}(2,1)-\delta$ $F_{i,j}(2,2)+\delta$ $F_{i,j}(2,3)-\delta$
$F_{i,j}(3,0)-\delta$ $F_{i,j}(3,1)+\delta$ $F_{i,j}(3,2)-\delta$ $F_{i,j}(3,3)+\delta$

図 8

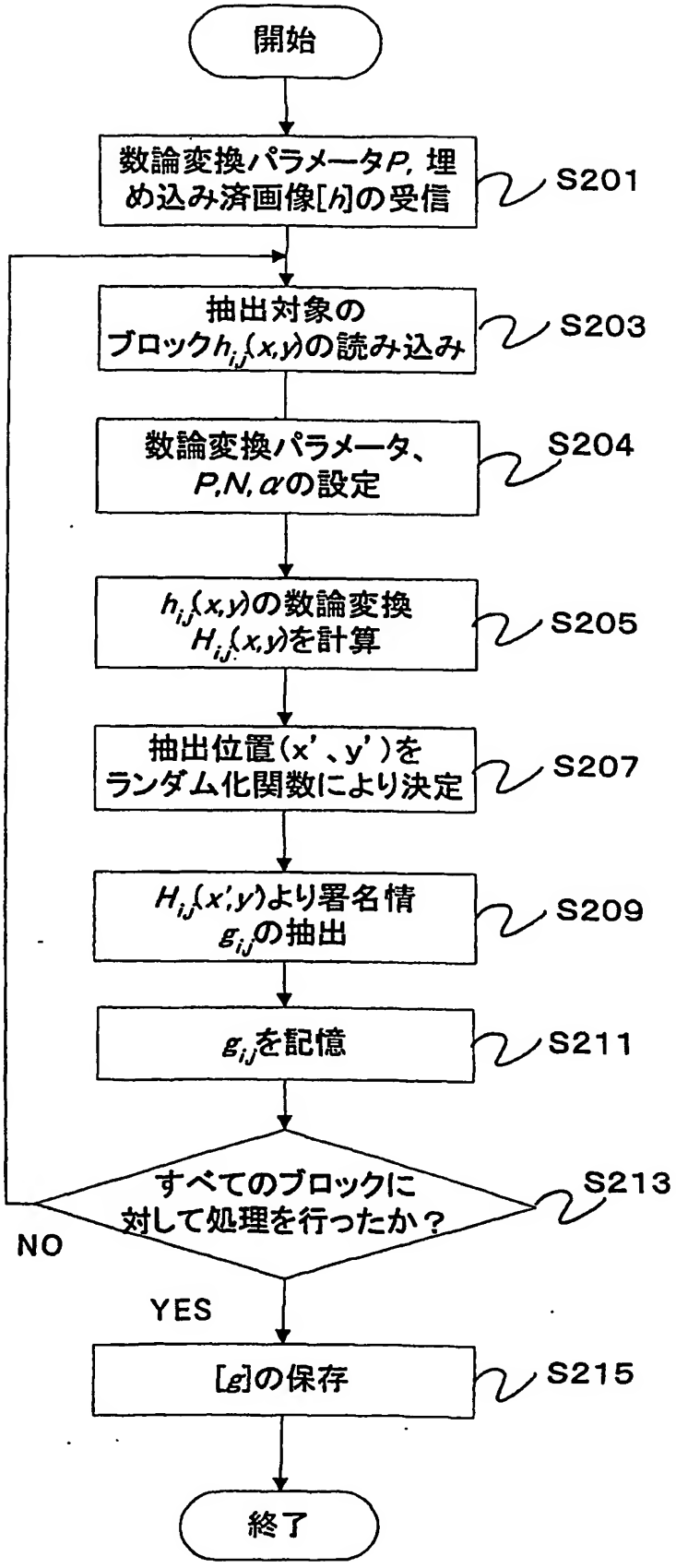
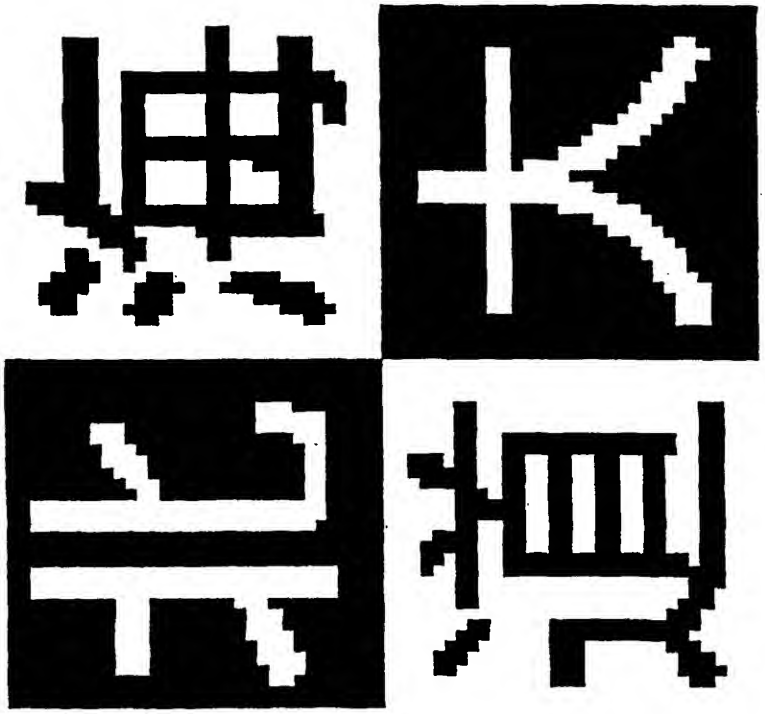
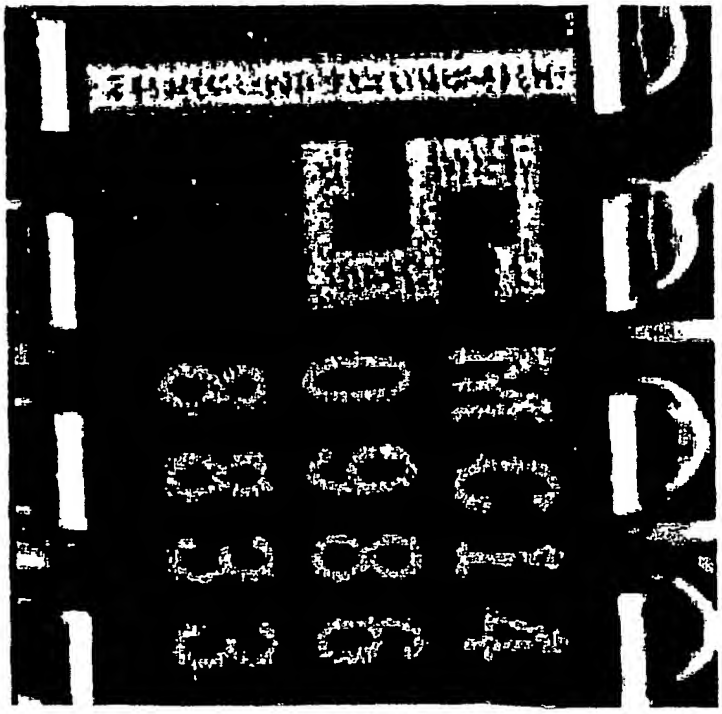

開始
数論変換パラメータP, 埋め込み済画像[h]の受信
S201
抽出対象のブロック$h_{i,j}(x,y)$の読み込み
S203
数論変換パラメータ、P,N,αの設定
S204
$h_{i,j}(x,y)$の数論変換$H_{i,j}(x,y)$を計算
S205
抽出位置(x'、y')をランダム化関数により決定
S207
$H_{i,j}(x',y')$より署名情$g_{i,j}$の抽出
S209
$g_{i,j}$を記憶
S211
すべてのブロックに対して処理を行ったか？
S213
NO
YES
[g]の保存
S215
終了

図９



(b)



(a)

図10

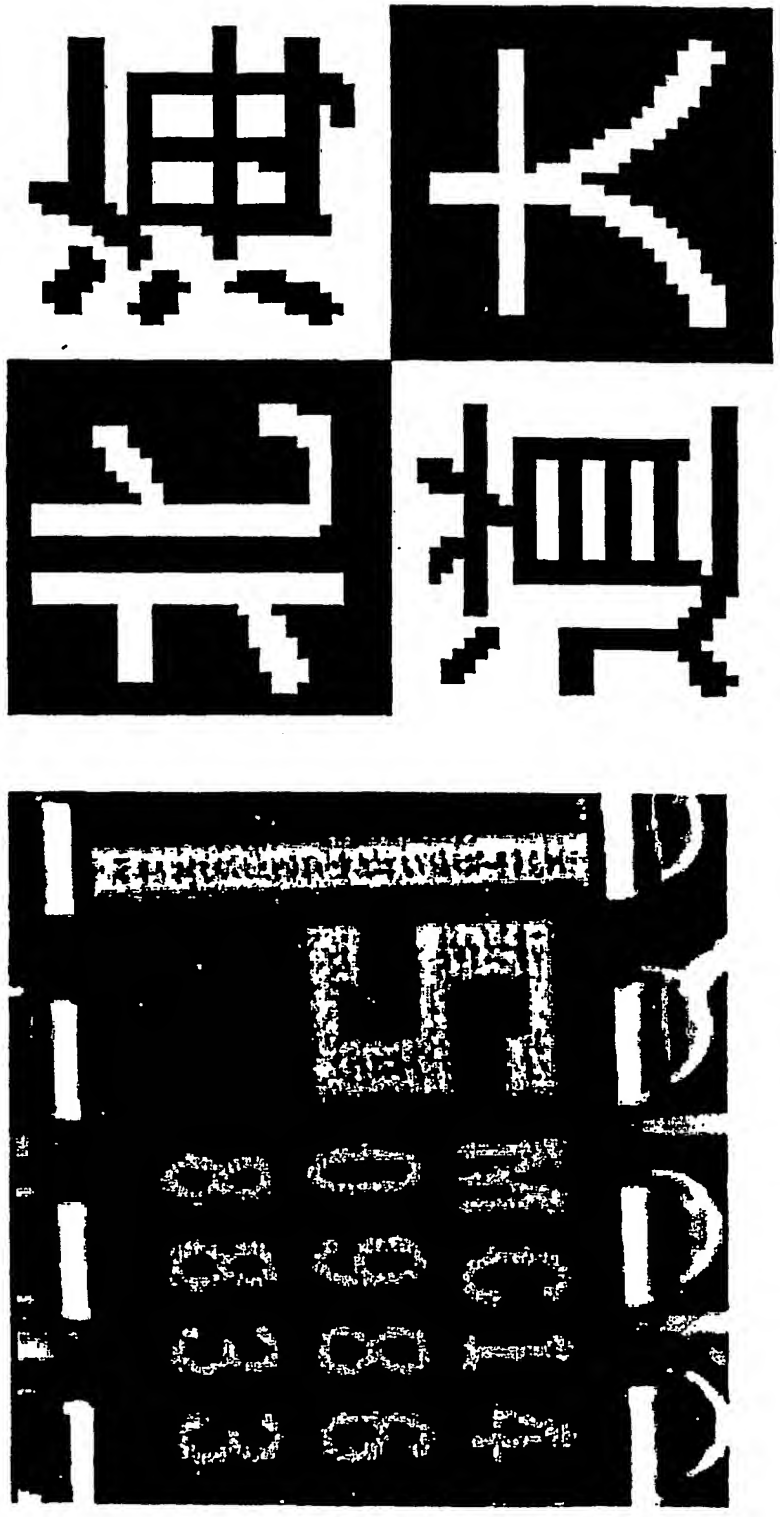


図11

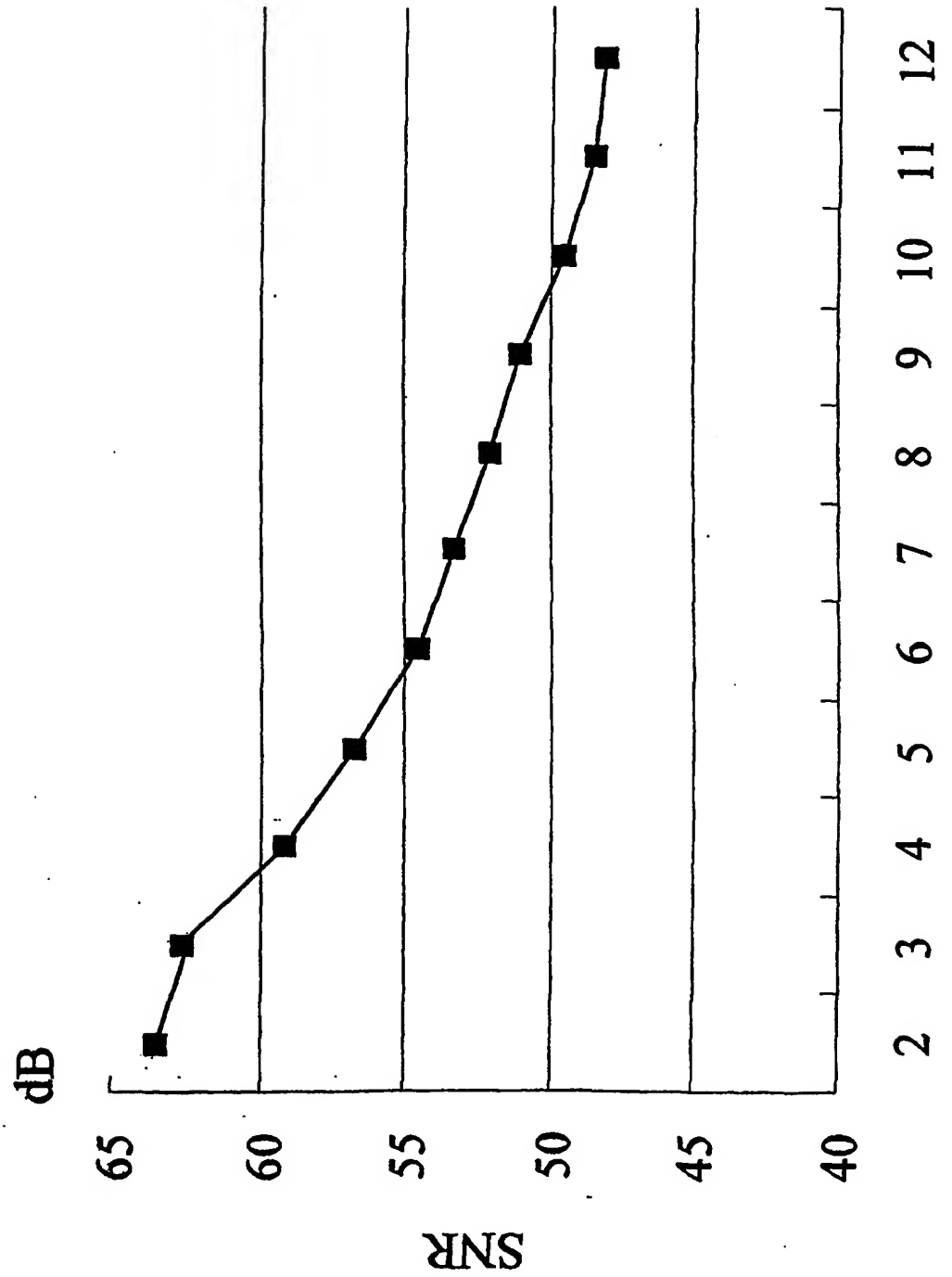
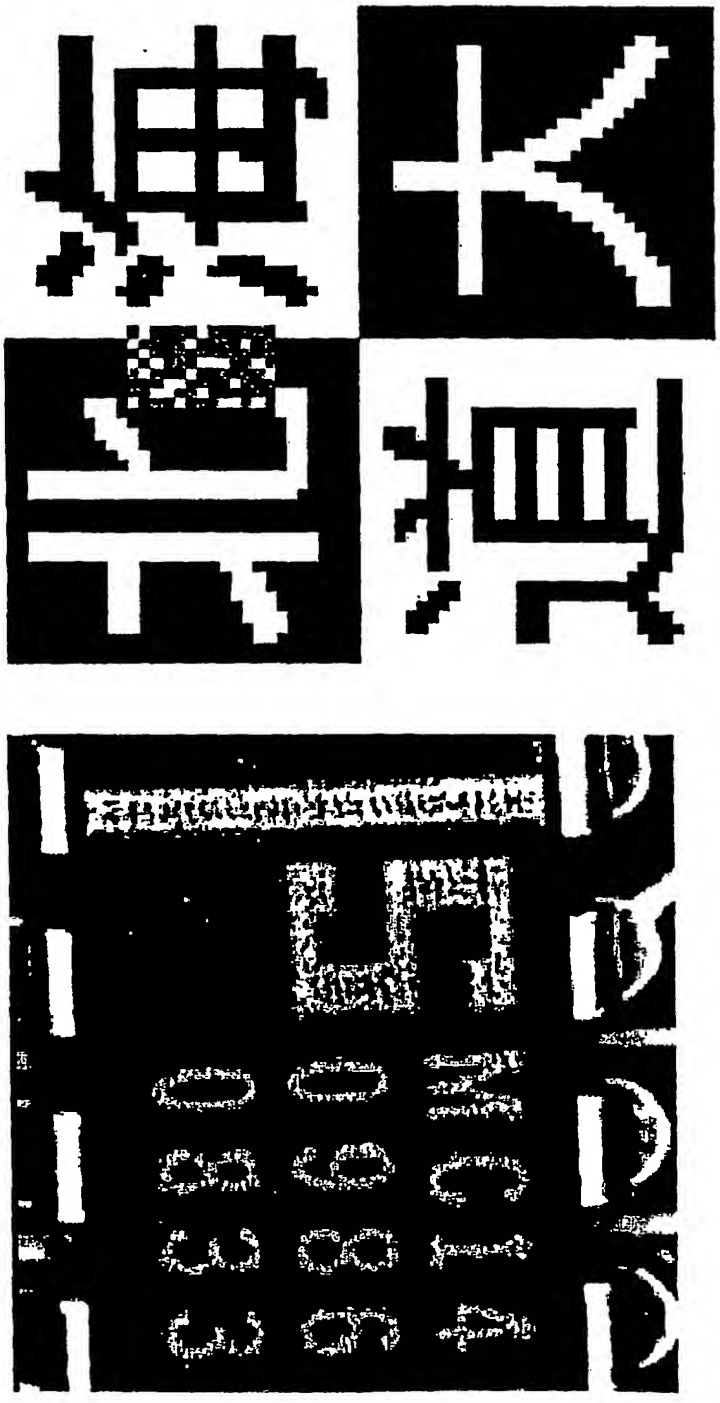


図12



(a) (b)

図13

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP03/13772

A. CLASSIFICATION OF SUBJECT MATTER
Int.Cl[7] H04N1/387

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
Int.Cl[7] H04N1/387

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Jitsuyo Shinan Koho	1922-1996	Toroku Jitsuyo Shinan Koho	1994-2003
Kokai Jitsuyo Shinan Koho	1971-2003	Jitsuyo Shinan Toroku Koho	1996-2003

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	Hideaki TAMORI et al., "Suron Henkan o Mochiita Kaizan Kenshutsu Kano na Denshi Sukashi Hoshiki", The Institute of Electronics, Information and Communication Engineers Gijutsu Kenkyu Hokoku, IE2001-33, 01 July, 2001 (01.07.01), pages 105 to 110	1-20
X	Hideaki TAMORI et al., "Suron Henkan ni yoru Zeijakugata Denshi Sukashi o Mochiita Seishi Gazo no Kaizan Ichi Kenshutsu Kano to Kaizan Teisei", The Institute of Electronics, Information and Communication Engineers Gijutsu Kenkyu Hokoku, IE2002-45, 01 July, 2002 (01.07.02), pages 19 to 24	1-20

[X] Further documents are listed in the continuation of Box C. [ ] See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier document but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search 02 December, 2003 (02.12.03)	Date of mailing of the international search report 16 December, 2003 (16.12.03)
Name and mailing address of the ISA/ Japanese Patent Office Facsimile No.	Authorized officer Telephone No.

Form PCT/ISA/210 (second sheet) (July 1998)

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP03/13772

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	JP 2002-44429 A (Kowa Co., Ltd.), 08 February, 2002 (08.02.02), Full text (Family: none)	1-3,15-20
A	JP 2001-148778 A (Canon Inc.), 29 May, 2001 (29.05.01), Full text (Family: none)	1-3,15-20
A	JP 2000-228632 A (Sony Corp.), 15 August, 2000 (15.08.00), Full text (Family: none)	1-3,15-20

国際調査報告

国際出願番号 PCT／JP03／13772

A. 発明の属する分野の分類（国際特許分類（IPC））

Int. Cl⁷ H04N1／387

B. 調査を行った分野

調査を行った最小限資料（国際特許分類（IPC））

Int. Cl⁷ H04N1／387

最小限資料以外の資料で調査を行った分野に含まれるもの

日本国実用新案公報	1922－1996年
日本国公開実用新案公報	1971－2003年
日本国登録実用新案公報	1994－2003年
日本国実用新案登録公報	1996－2003年

国際調査で使用した電子データベース（データベースの名称、調査に使用した用語）

C. 関連すると認められる文献

引用文献のカテゴリー＊	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する請求の範囲の番号
X	田森秀明他，数論変換を用いた改ざん検出可能な電子透かし方式，電子情報通信学会技術研究報告ＩＥ２００１－３３，２００１．０７．０１，p．１０５－１１０	１－２０
X	田森秀明他，数論変換による脆弱型電子透かしを用いた静止画像の改ざん位置検出可能と改ざん訂正，電子情報通信学会技術研究報告ＩＥ２００２－４５，２００２．０７．０１，p．１９－２４	１－２０

☒ C欄の続きにも文献が列挙されている。　☐ パテントファミリーに関する別紙を参照。

＊ 引用文献のカテゴリー
「A」特に関連のある文献ではなく、一般的技術水準を示すもの
「E」国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの
「L」優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献（理由を付す）
「O」口頭による開示、使用、展示等に言及する文献
「P」国際出願日前で、かつ優先権の主張の基礎となる出願の日の後に公表された文献
「T」国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの
「X」特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの
「Y」特に関連のある文献であって、当該文献と他の１以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの
「&」同一パテントファミリー文献

国際調査を完了した日 02．12．03	国際調査報告の発送日 16.12.03
国際調査機関の名称及びあて先 日本国特許庁（ISA／JP） 郵便番号１００－８９１５ 東京都千代田区霞が関三丁目４番３号	特許庁審査官（権限のある職員） 仲間 晃　印　5V　3359 電話番号 03－3581－1101 内線 3571

様式PCT／ISA／210（第2ページ）（1998年7月）

C（続き）．　関連すると認められる文献

引用文献のカテゴリー＊	引用文献名　及び一部の箇所が関連するときは、その関連する箇所の表示	関連する請求の範囲の番号
A	ＪＰ ２００２－４４４２９　Ａ（興和株式会社）２００２．０２．０８，全文（ファミリーなし）	１－３，１５－２０
A	ＪＰ ２００１－１４８７７８　Ａ（キャノン株式会社）２００１．０５．２９，全文（ファミリーなし）	１－３，１５－２０
A	ＪＰ２０００－２２８６３２　Ａ（ソニー株式会社）２０００．０８．１５，全文（ファミリーなし）	１－３，１５－２０